

March 2011

COMBATING CHILD PORNOGRAPHY

Steps Are Needed to
Ensure That Tips to
Law Enforcement Are
Useful and Forensic
Examinations Are
Cost Effective



G A O

Accountability * Integrity * Reliability

Why GAO Did This Study

The Department of Justice (DOJ) reports that online child pornography crime has increased. DOJ funds the National Center for Missing and Exploited Children (NCMEC), which maintains the CyberTipline to receive child pornography tips. The Providing Resources, Officers, and Technology To Eradicate Cyber Threats to Our Children Act of 2008 (the Act) contains provisions to facilitate these investigations and create a national strategy to prevent, among other things, child pornography. The Act directed GAO to report on actions to minimize duplication and enhance federal expenditures to address this crime. This report examines (1) the extent to which NCMEC determines the usefulness of tips; (2) mechanisms to help law enforcement coordination (i.e., deconfliction); and (3) the extent to which agencies are addressing factors that federal law enforcement reports may inhibit investigations. GAO analyzed the Act and spoke to law enforcement officials who investigate these crimes, selected to reflect geographic range, among other things. Although these interviews cannot be generalized, they provided insight into investigations.

What GAO Recommends

GAO recommends that NCMEC enhance its processes to collect feedback to improve tips and that DOJ assess the costs and benefits of steps agencies take to ensure the integrity of forensic analysis. NCMEC and DOJ generally concurred with our recommendations and discussed actions to address them.

View [GAO-11-334](#) or key components. For more information, contact Eileen Larence at (202) 512-8777 or larencee@gao.gov.

COMBATING CHILD PORNOGRAPHY

Steps Are Needed to Ensure That Tips to Law Enforcement Are Useful and Forensic Examinations Are Cost Effective

What GAO Found

NCMEC takes steps to obtain feedback from law enforcement on the usefulness of CyberTipline reports; however, it does not systematically collect information on how useful individual reports are for initiating and advancing investigations or about information gaps that limit reports' usefulness. For instance, NCMEC solicits feedback via e-mail or in person quarterly from federal law enforcement liaisons at NCMEC about the overall usefulness of CyberTipline reports. However, according to many law enforcement officials GAO contacted, information in a CyberTipline report may not contain an image of apparent child pornography or may contain old data. NCMEC officials said that they are interested in obtaining additional feedback to enhance the usefulness of its reports and could explore additional methods to gather such information, such as creating a systematic process for obtaining feedback from federal law enforcement. Enhancing its processes for collecting feedback on the usefulness of CyberTipline reports could help NCMEC ensure that reports are as useful as possible to law enforcement.

Existing deconfliction mechanisms generally prevent pursuit of the same suspects but are fragmented; DOJ is in the early stages of developing a system to address this fragmentation. Many law enforcement officials GAO contacted reported using various nonautomated (e.g., task forces) and automated (e.g., investigative systems) mechanisms to avoid duplication of effort in investigations. But these officials reported that there is not a single automated system that provides comprehensive case information and deconfliction, which can contribute to difficulties coordinating investigations. As mandated in the Act, DOJ is developing a national system to, among other things, provide law enforcement with a single deconfliction tool. Specifically, DOJ is conducting a needs assessment—which it plans to complete in 12 to 24 months—to use as a basis for system development. However, because DOJ is waiting on the results of the needs assessment to begin system development, it may be several years before the system is operational.

Backlogs in the forensic analysis of digital evidence can delay or hinder online child pornography investigations; assessing the costs and benefits of taking extra steps to ensure the integrity of forensic analysis could help determine if there are efficiencies that could reduce backlogs. Forensic analysis of digital evidence consists of the review of information from digital media, such as hard drives, and can prove online child pornography crime. Several factors may contribute to backlogs in forensic analysis, including the steps federal law enforcement agencies believe enhance the integrity of analysis, such as making exact copies of digital evidence to discourage tampering. The FBI takes additional steps it believes enhance integrity, such as separating the forensic examination from the investigation. However, some federal officials and prosecutors GAO spoke with differed on the need for such steps. According to DOJ, the national strategy's working group is in a good position to address backlog issues and having this group assess the costs and benefits of steps taken to ensure the integrity of forensic analysis could help it determine potential efficiencies that could reduce backlogs.

Contents

Letter		1
	Background	8
	DOJ Has To Take Action on Three Remaining Responsibilities under the Act	12
	NCMEC Provided ESPs Reporting Guidance and Online Detection Information	15
	Expanding Feedback from Law Enforcement Could Help Improve the Usefulness of CyberTipline Reports and Better Address Increasing Number of Reports	20
	Existing Deconfliction Mechanisms, While Fragmented, Generally Prevent Pursuit of the Same Suspects; DOJ Is Starting to Develop a National System	28
	Backlogs in Forensic Analysis of Digital Evidence and Length of Time ESPs Retain User Data Can Hinder Investigations	33
	Conclusions	45
	Recommendations	46
	Agency Comments, Third Party Views, and Our Evaluation	47
Appendix I	Key Federal Agencies Involved in Combating Online Child Pornography	50
Appendix II	Status of Efforts of DOJ and NCMEC’s CyberTipline to Implement Provisions of the PROTECT Our Children Act of 2008	58
Appendix III	Overview of NIDS Components and System Functions Outlined by the PROTECT Our Children Act of 2008	67
Appendix IV	Comments from the Department of Justice	68
Appendix V	Comments from the National Center for Missing and Exploited Children	70

Tables

Table 1: Federal Agencies Involved in Combating Child Pornography	10
Table 2: Overview of Process Different Federal Agencies with Liaisons at NCMEC Use to Review and Forward CyberTipline Reports for Investigation	23
Table 3: FBI Personnel Dedicated to Combating Child Exploitation	50
Table 4: FBI Resources Obligated for Combating Child Exploitation	51
Table 5: Number of FBI Child Pornography Investigations and Arrests	51
Table 6: CEOS Personnel Dedicated for Combating Child Exploitation and Obscenity Offenses	52
Table 7: CEOS Funds Obligated for Combating Federal Child Exploitation and Obscenity Offenses	52
Table 8: Number of ICAC Task Force Child Exploitation Cases Investigated and Arrests	53
Table 9: ICE Personnel Dedicated for Combating Child Exploitation	55
Table 10: ICE Resources Obligated for Combating Child Exploitation	55
Table 11: Number of Child Pornography Cases Initiated and Arrests by ICE Agents	55
Table 12: Number of USSS Investigations and Arrests Related to Child Pornography	56
Table 13: Full Time and Part Time Postal Inspectors Assigned to Child Exploitation Investigations	57
Table 14: Postal Inspection Service Investigations and Arrests Related to Child Exploitation and Child Pornography	57
Table 15: Status of Efforts of the Attorney General and NCMEC's CyberTipline to Implement Their Responsibilities under the PROTECT Our Children Act of 2008	58
Table 16: Information on the NIDS Components Required by and Functions Described in the PROTECT Our Children Act of 2008	67

Figures

Figure 1: Number of Arrests by ICAC Task Forces and Federal Law Enforcement Agencies Involved in Online Child Exploitation and Child Pornography Investigations from Fiscal Years 2006 through 2010	12
Figure 2: Overview of NCMEC Process for Receiving and Disseminating CyberTipline Reports	21

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



G A O

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

March 31, 2011

The Honorable Patrick J. Leahy
Chairman
The Honorable Charles E. Grassley
Ranking Member
Committee on the Judiciary
United States Senate

The Honorable Lamar S. Smith
Chairman
The Honorable John Conyers, Jr.
Ranking Member
Committee on the Judiciary
House of Representatives

The Internet, while changing the way our society communicates, has also changed the nature of many crimes, including online child pornography. According to the Department of Justice's (DOJ) National Strategy for Child Exploitation Prevention and Interdiction (National Strategy), the numbers of child pornography images traded on the Internet, child pornography offenders, and children victimized by child pornography have dramatically increased.¹ For example, Internet Crimes Against Children (ICAC) task forces reported an increase of about 150 percent in the number of arrests for child pornography-related offenses, from about 2,100 in fiscal year 2006 to about 5,300 in fiscal year 2010.² Similarly, since fiscal year 2006, the number of defendants prosecuted by U.S. Attorneys' Offices for child exploitation crime, including online child pornography, increased by 35 percent, with 2,250 indictments against 2,367 defendants filed in fiscal year

¹*The National Strategy for Child Exploitation Prevention and Interdiction, A Report to Congress*, U.S. Department of Justice, August 2010.

²The ICAC Task Force Program is a network of 61 task forces comprised of federal, state, local, and tribal law enforcement and prosecutorial agencies. ICAC task force agencies engage in investigations, forensic examinations, and prosecutions of Internet crimes against children.

2010.³ These crimes carry severe penalties. For example, for the first offense, possessing child pornography may result in imprisonment of up to 10 years; receiving, selling, or distributing child pornography may result in imprisonment of at least 5 years and up to 20 years; and producing child pornography may result in imprisonment of at least 15 years and up to 30 years.⁴ Further, the offenders who commit child pornography crimes often pose a physical threat to children. According to DOJ's National Strategy, analysis of federally prosecuted child pornography cases indicates contact offenses against children, such as the sexual abuse of a minor, were discovered in approximately one-third of all cases.

Digital cameras and computers have made it easier for offenders to produce and distribute child pornography because they can bypass print shops and upload photos from their cameras directly to the Internet. In addition, the increased sophistication of offenders in the production and distribution of child pornography and the use of advanced technologies to avoid detection has made it more difficult for law enforcement to detect their activities and identify suspects who attempt to hide their identifying information.

In response to the increase in online child pornography crime, multiple federal law enforcement agencies have developed specialized units to address crimes against children, and Congress has passed legislation requiring greater coordination on, and authorizing an increase in resources available to address, these crimes. For example, due to the increase in the number of investigations that involved sex offenders using computers to share pornographic images of minors, in 1995 the Federal Bureau of Investigation (FBI) developed the Innocent Images National Initiative (Innocent Images), which teams FBI agents and local police in task forces to conduct undercover investigations of suspected offenders. Similarly,

³Pursuant to the Providing Resources, Officers, and Technology To Eradicate Cyber Threats to Our Children Act of 2008 (PROTECT Our Children Act of 2008), "child exploitation" generally consists of conduct involving a minor that violates specific criminal provisions of the U.S. Code, or any sexual activity involving a minor for which a person can be charged with a criminal offense. Pub. L. No. 110-401, § 2, 122 Stat. 4229, 4230. Some of these criminal provisions include, for example, causing a minor to engage in a sex act by force; transporting an individual for purposes of prostitution or other criminal sexual activity; or mailing, receiving, and distributing child pornography. Child pornography has a more specific definition under 18 U.S.C. § 2256, and generally consists of any visual depiction, the production of which involves the use of a minor engaging in sexually explicit conduct or that involves a minor engaging in sexually explicit conduct.

⁴18 U.S.C. §§ 2251, 2252, 2252A.

Immigration and Customs Enforcement (ICE), which enforces trans-border violations of federal child exploitation statutes and works to, among other things, prevent the introduction of prohibited contraband, such as child pornography, into the United States, initiated its Cyber Crimes Center in 1997. Finally, the United States Postal Inspection Service (USPIS) has 45 specially trained inspectors located in its field divisions who investigate crimes related to the exploitation of children and have jurisdiction over these types of crimes that involve the mail. To assist these law enforcement efforts, DOJ's Office of Juvenile Justice and Delinquency Prevention (OJJDP) allocates funds to the National Center for Missing and Exploited Children (NCMEC), which serves as a national resource center for information related to crimes against children.⁵ The center also maintains the CyberTipline to receive tips on child pornography from electronic service providers (ESP) and members of the general public.⁶ In addition to federal efforts to address these crimes, state and local law enforcement agencies generally enforce child pornography laws within their own jurisdictions and may work collaboratively with federal agencies through federal task forces to combat child pornography.

More recently, Congress passed the Providing Resources, Officers, and Technology To Eradicate Cyber Threats to Our Children Act of 2008 (PROTECT Our Children Act of 2008, or the Act) which requires, among other things, that the Attorney General create and implement a National Strategy for Child Exploitation Prevention and Interdiction.⁷ The National Strategy, published in August 2010, has the goal of preventing child sexual exploitation from occurring. The Act also requires that ESPs report to NCMEC any instances of apparent child pornography that they become aware of on their networks. In addition, the Act requires the Attorney

⁵The Missing Children's Assistance Act, as amended, directs OJJDP to make an annual grant to NCMEC to carry out various responsibilities related to missing and exploited children. Among these are coordinating public and private programs to locate missing children, providing technical assistance and training, and providing information and assistance services. 42 U.S.C. § 5773(b)(1).

⁶The PROTECT Our Children Act of 2008 requires electronic communication service providers and remote computing service providers to make reports to the CyberTipline. Pub. L. No. 110-401, § 501(a) (codified at 18 U.S.C. § 2258A). Collectively termed ESPs for purposes of this report, these include any service that provides to users the ability to send or receive wire or electronic communications, such as e-mail and instant messaging services and gateway access to the Internet; as well as data storage services, such as those that offer subscribers the opportunity to store materials like address books, calendars, photo albums, video content, electronic files, documents, and other types of content.

⁷Pub. L. No. 110-401, 122 Stat. 4229.

General to establish a National Internet Crimes Against Children Data System (NIDS) to serve as, among other things, a platform to conduct undercover investigations of child exploitation crime and a centralized system for deconfliction for federal, state, and local law enforcement.⁸

The Act also directs us to report on, among other things, the efforts of the Attorney General and NCMEC's CyberTipline in carrying out their responsibilities under the Act. In addition, it directs us to report on actions taken to minimize duplication and enhance the expenditure of federal resources in enforcing, investigating, and prosecuting child pornography crimes. Specifically, this report addresses the following questions:

- To what extent have DOJ and the CyberTipline implemented their responsibilities under the Act?
- What information does NCMEC provide to ESPs to facilitate reporting of apparent online child pornography to the CyberTipline?
- To what extent does NCMEC have mechanisms in place to help determine how useful law enforcement agencies find the CyberTipline incident information and services that it provides for initiating online child pornography investigations?
- What deconfliction mechanisms exist that help prevent law enforcement agencies from pursuing the same suspected online child pornography offenders or interfering with each other's investigations, and to what extent, if any, could these mechanisms be improved?
- What factors, if any, did federal law enforcement agencies report as limiting their ability to investigate and prosecute suspected online child pornography offenders, and to what extent are agencies addressing these factors?

For all objectives, we analyzed the Act, which outlines requirements for DOJ, NCMEC, and ESPs, and the National Strategy, which, among other things, describes information on threats to children and reviews law enforcement coordination efforts and federal forensic analysis programs. We also analyzed data from fiscal year 2006 through fiscal year 2010 on the number of investigations and arrests by federal law enforcement agencies and ICAC task forces to assess trends in child exploitation and child

⁸Deconfliction is the coordination and information sharing among law enforcement agencies on multijurisdiction investigations to help ensure officer safety and the effective use of resources.

pornography cases.⁹ To assess the extent to which DOJ and NCMEC have implemented their responsibilities under the Act, we interviewed DOJ's National Coordinator for Child Exploitation Prevention and Interdiction, the senior official responsible for coordinating the development of the National Strategy, and NCMEC officials to discuss efforts to implement the Act's provisions. We compared these efforts with criteria in standard practices for program management.¹⁰

To identify the information NCMEC provides to ESPs to facilitate reporting of apparent online child pornography, we assessed documentation NCMEC provides to ESPs, such as its guide for reporting to the CyberTipline, and interviewed officials from NCMEC. To obtain information on any concerns ESPs had about reporting to the CyberTipline, we interviewed officials from a nonprobability sample of 19 ESPs, which we selected from among the 620 ESPs that had registered with NCMEC as of April 2010.¹¹ We selected these 19 ESPs to reflect a range of geographic locations, types of service provided, number of tips submitted to the CyberTipline, and number of child pornography investigations referred to and accepted for prosecution in the judicial district in which the ESP was located. Their comments cannot be generalized to all ESPs; however, the interviews provided perspectives from ESPs about reporting to the CyberTipline. We also interviewed officials from three civil liberties organizations—the American Civil Liberties Union, the Electronic Frontier Foundation, and the Center for Democracy and Technology—to obtain information about privacy

⁹We chose these dates to obtain an overview of trends in law enforcement activity related to efforts to combat online crimes against children as well as to examine federal activity before and after passage of the PROTECT Our Children Act of 2008. Specifically, we analyzed data on investigations and arrests from FBI, ICE, United States Secret Service, and USPIS; resource data from FBI, DOJ's Child Exploitation and Obscenity Section, ICE, and USPIS; and data on cases and investigations reported by ICAC task forces to OJJDP. To assess the reliability of these data, we questioned officials knowledgeable on their respective agency's data systems about how the data were compiled and the steps taken to ensure data quality. Based on their responses, we determined these data to be sufficiently reliable for the purposes of this report.

¹⁰Program management standards we reviewed are reflected in the Project Management Institute's *The Standard for Program Management* © (2006).

¹¹NCMEC provides a Web page specifically for ESPs that have registered with NCMEC to allow for secured submission of CyberTipline reports. We selected ESPs from among the 620 that had registered as of April 2010 to reflect time before and after enactment of the Act.

concerns expressed by Internet consumers in response to ESPs' reporting activities.¹²

To assess the extent to which NCMEC has mechanisms in place to help determine how useful law enforcement agencies find CyberTipline information, we reviewed relevant documentation, such as NCMEC's feedback forms and training briefings about the CyberTipline. To determine trends in the use of the CyberTipline, we analyzed data on the number of reports submitted by ESPs and the general public and the number of these reports NCMEC made available to law enforcement from January 1, 2008, through December 31, 2010.¹³ We also interviewed the three federal law enforcement liaisons from the FBI, ICE, and USFIS located at NCMEC and officials from 8 of the 61 ICAC task forces about the usefulness of the CyberTipline reports and the services NCMEC provided. Specifically, we interviewed officials from ICAC task forces located in six federal judicial districts, which we selected to obtain geographic representation and based on the number of child pornography investigations referred to and accepted by U.S. Attorneys' Offices for prosecution.¹⁴ While the information obtained from these interviews cannot be generalized to all ICAC task forces or their members, the interviews provided a range of perspectives about how useful NCMEC's information and services were for initiating investigations. We compared the mechanisms NCMEC has in place with best practices articulated in our

¹²We selected these organizations based on their varied perspectives and focuses in civil liberties, high-technology, and partnerships with Internet and law enforcement communities. The information obtained from these interviews cannot be generalized to all such organizations; however, the interviews provided an overview of perspectives about Internet-related privacy concerns.

¹³We selected these dates to provide 2 full years of data from the time of our review, reflecting time before and after enactment of the Act. To assess the reliability of these data, we questioned NCMEC officials knowledgeable on the data about how the reports were compiled and the steps taken to ensure data quality. Based on their responses, we determined these data to be sufficiently reliable to report general trends.

¹⁴These ICAC task forces were located in the Middle District of Florida, the Western District of New York, the Western District of Missouri, the Northern District of California, the District of Arizona, and the Eastern District of Virginia. We also interviewed officials from two ICAC task forces, the Northern District of Texas and the Eastern District of Pennsylvania, which we selected based on their experience with an automated deconfliction tool and geographic location.

prior reports highlighting the importance of soliciting input from users and assessing whether the information disseminated is meeting users' needs.¹⁵

To determine what mechanisms prevent law enforcement agencies from pursuing the same offenders or interfering with each others' investigations, we assessed information on tools available to facilitate coordination and deconfliction, such as the ICAC Data Network Toolkit Manual, as well as memoranda of understanding between DOJ and agencies participating in the ICAC Task Force Program. We also reviewed OJJDP's fiscal years 2009 and 2010 grant solicitations for the NIDS project, the proposal for its development, and grant manuals, which outlined the agency's approach for system development. To discuss available mechanisms, we interviewed law enforcement officials who investigate child pornography offenders in the six judicial districts we selected. Specifically, we held 20 interviews with law enforcement officials from FBI, ICE, United States Secret Service (USSS), and USPIS; 8 interviews with officials from ICAC task forces; and 7 interviews with Assistant United States Attorneys (AUSA) who serve as coordinators for the Project Safe Childhood Initiative.¹⁶ The information obtained from these interviews is not generalizable to law enforcement officials or agencies in all judicial districts. However, it provided examples and perspectives about law enforcement's efforts to coordinate investigations and use deconfliction mechanisms.

To determine factors, if any, federal law enforcement agencies identified that limited their ability to investigate and prosecute suspected online child pornography offenders and to what extent agencies are addressing these factors, we included questions on this topic in our interviews with law enforcement officials from FBI, ICE, USSS, USPIS, and AUSAs. We also toured FBI, ICE, and USPIS digital forensic laboratories to observe their forensic processes. In addition, we interviewed prosecutors from the Child Exploitation and Obscenity Section (CEOS) who work directly with digital forensic examiners assigned to CEOS's High Technology

¹⁵For example, see GAO, *Transportation Research: Opportunities for Improving the Oversight of DOT's Research Programs and User Satisfaction with Transportation Statistics*, [GAO-06-917](#) (Washington, D.C.: Aug. 15, 2006).

¹⁶The initiative is a DOJ initiative designed to reduce the incidence of sexual exploitation of children. Among their responsibilities, coordinators interact with area law enforcement to reduce child exploitation. In addition to interviewing coordinators in the six selected districts, we interviewed AUSAs from a seventh district, selected to reflect geographic range.

Investigative Unit, which is collocated with CEOS prosecutors, to support investigations and prosecutions; officials from FBI's Innocent Images and Digital Evidence Section, which oversees forensic analysis of digital evidence; officials from ICE's Cyber Crimes Center; and officials from USPIS's Digital Evidence Unit, which is responsible for forensic analysis practices, on how these agencies are addressing the factors identified.¹⁷ We compared these efforts to guidance outlined by the Office of Management and Budget (OMB) for considering alternative means of achieving program objectives.¹⁸

We conducted this performance audit from September 2009 through March 2011 in accordance with generally accepted government auditing standards.¹⁹ Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

National Center for Missing and Exploited Children (NCMEC) and the CyberTipline

NCMEC is a private, nonprofit organization that serves as the nation's resource center for child protection. NCMEC's mission is to assist in the location and recovery of missing children and to prevent the abduction, molestation, sexual exploitation, and victimization of children. NCMEC is congressionally authorized to carry out certain tasks with grant funding it receives through a cooperative agreement with OJJDP.²⁰ According to NCMEC, for calendar year 2009, NCMEC received about 77 percent of its funding from federal sources, with the remainder coming from other revenue and support, such as corporate and private donations. From fiscal

¹⁷Within DOJ's Criminal Division, CEOS attorneys prosecute federal child exploitation offenses, including child pornography crimes, and provide prosecutorial guidance to federal law enforcement agencies, among other things.

¹⁸See Circular No. A-11 *Preparation, Submission, and Execution of the Budget* (July 2010); Circular No. A-94 *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs* (October 1992); and Circular A-4 *Regulatory Analysis* (September 2003).

¹⁹We briefed the reporting committees in October 2010 to meet time frames specified in the Act.

²⁰See 42 U.S.C. § 5773(b)(1).

years 2008 through 2010, NCMEC operated the CyberTipline at a cost of about \$7.6 million, an average of \$2.5 million per year excluding support by computer programmers.

In support of its mission and consistent with the Missing Children's Assistance Act, NCMEC maintains a 24-hour, toll-free telephone tipline for leads from individuals reporting the sexual exploitation of children and information on the possession, manufacture, or distribution of child pornography. NCMEC also coordinates public and private programs to locate missing children; offers technical assistance, training, and consultation to law enforcement agencies; and has developed specialized training programs and materials for law enforcement personnel.

NCMEC also maintains the CyberTipline to receive tips on child pornography from ESPs, which are required under the Act to report to NCMEC any instances when they become aware of apparent child pornography on their networks, as well as from the general public.²¹ ESPs that have registered with NCMEC can provide reports to the CyberTipline through a secure reporting form.²² NCMEC reported that as of December 31, 2010, 738 ESPs had registered out of an estimated 5,000 ESPs. According to NCMEC officials, it is difficult to identify the total number of ESPs or those that have not registered with NCMEC because there is no single source or list of the universe of ESPs. Based on our discussions with ESPs, they vary by types of services provided, ranging from access points to the Internet, search engines, and classified advertisements, to social networking sites. They may offer paid and free services, and have thousands or millions of customers. NCMEC reported that from January 1,

²¹See Pub. L. No. 110-401, § 501(a) (codified at 18 U.S.C. § 2258A). Before the passage of the PROTECT Our Children Act of 2008, ESPs were required to report instances of apparent child pornography to the CyberTipline under 42 U.S.C. § 13032(b), which provided for civil penalties for failure to report.

²²NCMEC maintains a secure Web page available specifically for registered ESPs as well as a Web page available for the general public, both of which allow for reports to be made to the CyberTipline. According to NCMEC officials, ESPs can also submit child pornography-related tips to the general public's Web page, in which case NCMEC contacts the ESP to register them so that future tips can be submitted to the ESP secure Web page.

2008, through December 31, 2010, 194 registered ESPs made about 248,000 reports to the CyberTipline.²³

Federal Law Enforcement Agencies Involved in Combating Online Child Pornography

As shown in table 1, several federal law enforcement agencies are involved in, and have specific units devoted to, combating online child pornography.

Table 1: Federal Agencies Involved in Combating Child Pornography

Department	Component	Law enforcement effort
DOJ	FBI	Proactively investigates crimes against children. Crimes Against Children Unit coordinators are located in each of the 56 field offices. Also has Innocent Images to combat Internet-related sexual exploitation of children.
	CEOS, within the Criminal Division	Prosecutes federal child sexual exploitation offenses, including child pornography crimes, enticement of children for sexually predatory purposes, transportation of offenders or children across state lines for sexually predatory purposes, domestic sex trafficking of children, and child sex tourism. Provides prosecutorial guidance to federal law enforcement agencies and U.S. Attorneys' Offices nationwide. Also develops and refines policies, legislative proposals, government practices, and agency regulations in the areas of sexual exploitation of minors.
	94 United States Attorneys' Offices	Prosecutes federal child exploitation-related cases.
	OJJDP	Allocates funds and administers the ICAC Task Force Program, which encourages multijurisdictional and multiagency responses to crimes against children involving the Internet.
Department of Homeland Security (DHS)	ICE, Cyber Crimes Center	Enforces trans-border violations of federal child exploitation statutes. Among other things, works to prevent the introduction of prohibited merchandise and contraband, such as child pornography, into the United States and investigates, interdicts, and prosecutes those individuals involved in possession, receipt, distribution, advertisement, transportation, and production of child pornography.
	USSS	Provides forensic and technical assistance in matters involving missing and sexually exploited children.
U.S. Postal Service	USPIS	Investigates child pornography and child sexual exploitation cases that involve U.S. mail, as well as Internet-related offenses in cases where mail is involved. The objective of the child exploitation program is to reduce and deter the use of the postal system for the procurement or delivery of materials that promote the sexual exploitation of children.

Source: GAO analysis of information provided by DOJ, DHS, and USPIS.

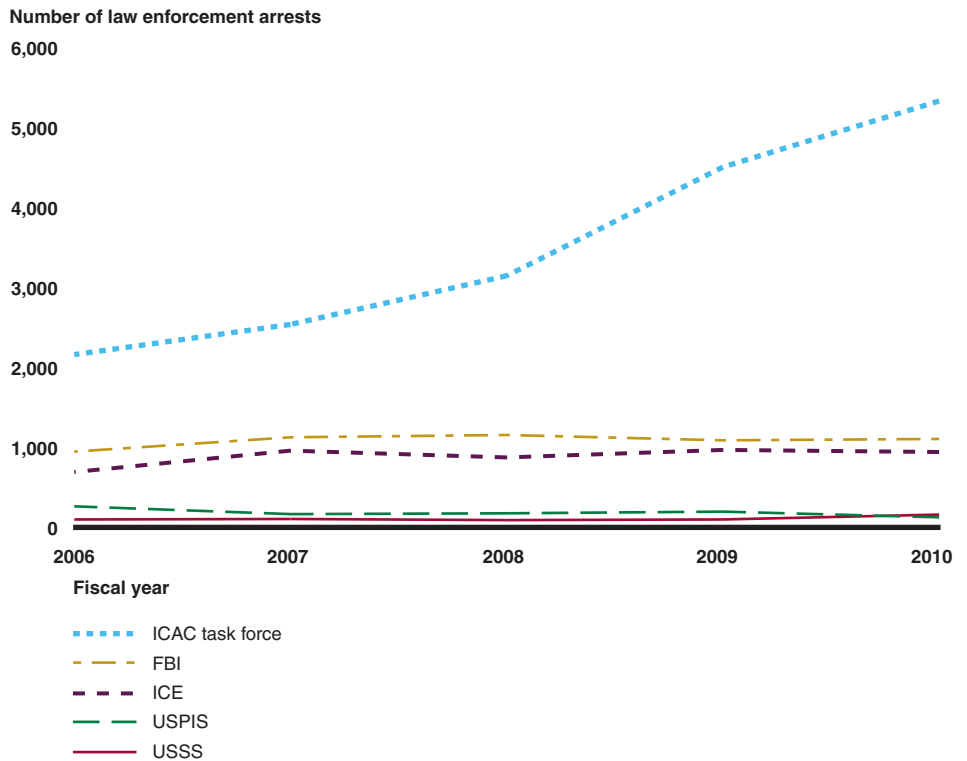
²³The number of reports submitted to the CyberTipline does not equate to the actual number of incidents of apparent child pornography being reported because, for example, different individuals may have reported the same incident to an ESP and each of these reports is recorded separately.

Appendix I provides additional details on the mission, role, level of resources, and numbers of investigations and arrests of these agencies.

Trends in the Number of Child Exploitation and Pornography Investigations

In its National Strategy, DOJ reported that the incidence of child exploitation, which, among other things, includes possessing, distributing, and producing child pornography, has been increasing since the 1990s, although the precise number of offenders accessing and trading child pornography material online is not known. For example, DOJ data show that from fiscal years 2006 through 2010, ICAC task forces estimate over an 80 percent increase in the number of complaints received from the public related to the possession, distribution, and manufacture of child pornography. These task forces also reported that arrests for child pornography have increased about 150 percent during the same period. FBI, ICE, and USSS reported increases in arrests of 17 percent, 37 percent, and 69 percent, respectively, from fiscal years 2006 through 2010. The USPIS reported a 54 percent decline in arrests for child pornography and child exploitation involving the U.S. mail. According to officials, this decline is, in part, due to the increased availability of child pornography through the Internet rather than the mail. Figure 1 shows the number of arrests made by ICAC task force investigators and federal law enforcement related to online child exploitation and child pornography from fiscal years 2006 through 2010.

Figure 1: Number of Arrests by ICAC Task Forces and Federal Law Enforcement Agencies Involved in Online Child Exploitation and Child Pornography Investigations from Fiscal Years 2006 through 2010



Source: GAO analysis of information provided by FBI, ICE, USPIIS, USSS, and OJJDP.

Note: Joint investigations between federal law enforcement agencies and ICAC task forces may be counted in both ICAC and federal investigative data. Although the extent is not known, DOJ officials said they believe the overlap is minimal.

DOJ Has To Take Action on Three Remaining Responsibilities under the Act

The Act, enacted in October of 2008, requires, among other things, that the Attorney General create and implement a National Strategy for Child Exploitation Prevention and Interdiction and contains provisions on the establishment of ICAC task forces. It also calls for the designation of a senior official at DOJ responsible for the National Strategy—the National Coordinator—who is to act as a liaison with other federal entities in the development of the strategy. In January 2010, DOJ selected a National Coordinator and in August 2010, to coincide with the publication of the National Strategy, formed the National Strategy Working Group to assist

with its implementation.²⁴ This Working Group consists of six subcommittees that address implementation of specific provisions of the strategy, such as examining means to reduce backlogs of forensic analysis or coordinating grant funding with DOJ missions.²⁵ The Act also establishes in law the ICAC Task Force Program, which is dedicated to developing responses to online enticement of children by sexual offenders, child exploitation, and child pornography. Currently, there are 61 task forces with at least one per state, as required by the Act. The Act also authorizes the Attorney General to award grants to these task forces, and in fiscal year 2010, OJJDP awarded approximately \$19 million to state and local law enforcement agencies.

The Act also contains provisions that require NCMEC to, among other things, minimize the number of NCMEC employees who are provided access to CyberTipline images and forward child pornography related tips to law enforcement to further investigations. According to NCMEC officials, since the passage of the Act, NCMEC has reduced the number of employees with access to CyberTipline images by 21 percent from 72 to 57 by removing access to images by employees who transfer from the NCMEC division that reviews CyberTipline reports to other divisions. NCMEC also created a “read only” level of access to the CyberTipline for employees whose job responsibilities require them to have access to CyberTipline information, but not images. The Act also requires NCMEC to provide information that relates to any apparent child pornography image of an identified child to federal, state, and local law enforcement involved in the investigation of child pornography crime. NCMEC has several initiatives underway to provide law enforcement such information. For example, according to NCMEC officials, it has established a portal that allows law enforcement agencies access to NCMEC’s systems to quickly identify hash values of identified child victims.²⁶ The portal separates out hash values of identified child victims from those who have not been identified so that law enforcement can quickly match hash values they

²⁴This working group includes participants from the FBI, CEOS, ICE, USFIS, five ICAC task forces, the Executive Office for United States Attorneys, the Department of Defense, and USSS.

²⁵The six subcommittees are Technical Assistance, Global Outreach, Community Outreach, Research and Grant Planning, Training, and Law Enforcement Collaboration.

²⁶In general, a portal is a Web site that serves as a starting point to other destinations or activities and provides information from different sources in a unified way. Hash values, also known as digital fingerprints, are computational values that serve as unique identifiers for electronic files, such as images, documents, or storage media such as hard drives.

receive during investigations against the database of image information. NCMEC officials said that they plan to continue to register additional law enforcement officers in 2011. Further information on DOJ's and NCMEC's status in implementing provisions of the Act is provided in appendix II.

However, to date, DOJ has yet to take action on three provisions of the Act.

- Specifically, the Act requires the National Institute of Justice within DOJ to prepare a report, not later than 1 year after enactment (i.e., October 2009), to identify the factors indicating whether the subject of an online investigation poses a high risk of harm to children.²⁷ According to senior DOJ officials, this report has not been initiated because funds have not been appropriated for this activity under the Act, and DOJ does not have plans or a time frame to conduct such a study. However, according to the National Coordinator, an examination of how such a study would be conducted would likely be considered by the Working Group as it moves forward.
- In addition, the Act requires the Attorney General to submit a report to the Judiciary Committees, not later than 12 months after enactment, on various features of the Act, including an assessment of the information-sharing structure established in response to the Act and data related to CyberTipline reports.²⁸ According to officials, DOJ has not prepared this report and does not yet have a time frame for completing it.
- Finally, the Act requires the Attorney General to designate, in consultation with the Secretary of State, foreign law enforcement agencies to receive CyberTipline reports from NCMEC, as well as specify the conditions under which a report may be forwarded to such foreign agencies.²⁹ The Act also requires the Attorney General to develop a process for foreign agencies to request assistance from federal law enforcement related to NCMEC's reports.³⁰ According to the National Coordinator, DOJ has not yet designated a list of foreign law enforcement agencies to which CyberTipline reports may be forwarded nor established a process for these agencies to request DOJ's assistance. Nevertheless, NCMEC officials said that the center currently refers CyberTipline reports to some foreign law enforcement agencies through ICE attaches, as necessary, as we

²⁷Pub. L. No. 110-401, § 401.

²⁸*Id.* § 502(a).

²⁹*Id.* § 501(a) (codified at 18 U.S.C. § 2258A(d)).

³⁰*Id.*

discuss later in this report. DOJ officials said that they plan to coordinate with NCMEC to determine how their designation would work best with NCMEC's current process, but has no time frames for doing so.

DOJ has taken action to implement many of the provisions in the Act, but DOJ has not yet completed three provisions for which it has responsibility and has no specific plans or time frames for doing so. Standard practices for program and project management state that specific desired outcomes or results, such as the implementation of these provisions, should be defined and documented in the planning process along with the appropriate milestones and time frames needed to achieve those results.³¹ By defining the steps necessary to achieve these three provisions along with appropriate time frames for completion, DOJ could better ensure that it will comply with the law and be able to obtain information that may allow it to better protect the public and further investigations. Specifically, information on the danger posed by individuals being investigated for online child pornography crime could help law enforcement agencies allocate investigative resources towards those suspects most likely to pose a risk to the public. Similarly, an assessment of the information-sharing structure and data from the CyberTipline and the designation of foreign law enforcement agencies to receive NCMEC reports could speed the process of disseminating these reports, which may facilitate investigations conducted by these agencies.

NCMEC Provided ESPs Reporting Guidance and Online Detection Information

NCMEC Has Developed a Guide to Address ESPs' Concerns about Reporting Apparent Online Child Pornography

To help ESPs fulfill their responsibilities under law, NCMEC provides information to ESPs to address their concerns related to reporting apparent online child pornography to NCMEC's CyberTipline. Under the Missing Children's Assistance Act, NCMEC is authorized to operate a CyberTipline to provide ESPs with an effective means of reporting apparent Internet-related child sexual exploitation.³² The Act explicitly

³¹Project Management Institute, *The Standard for Program Management* © (2006).

³²42 U.S.C. § 5773(b)(1)(P).

does not require ESPs to monitor their networks to detect apparent child pornography, but it requires ESPs to report the facts and circumstances of incidents of apparent child pornography, of which they become aware, to the CyberTipline.³³ ESPs may become aware of apparent child pornography on their networks through passive means, such as receiving reports from users, or through active means, such as having personnel search for images on their networks or by monitoring chat rooms to detect instances when users may be trading illegal images. ESPs may also become aware of child pornography through technical means, such as using specialized software to detect and remove illegal files from their systems.

Officials we interviewed from 18 of the 19 ESPs expressed concerns about making reports of apparent child pornography to the CyberTipline in fulfillment of their responsibilities under the Act.³⁴ These concerns included:³⁵

- **Cost:** Officials to whom we spoke from 16 of the 19 ESPs expressed concerns about the costs associated with reporting or monitoring their networks for apparent child pornography. According to officials from 4 of these 16 ESPs, devoting staff and resources to review and report apparent child pornography can be costly. Officials from 1 ESP reported that it cost \$500,000 to develop a system to automate reporting to NCMEC—a reporting system they said was necessary to address the volume of instances of apparent child pornography encountered on the ESP’s network. Additionally, officials from 13 of the 19 ESPs we spoke with said that establishing methods to detect apparent child pornography, while not required, can be costly to implement. For example, 4 of these ESPs said it was costly to search for key words, check their computer network for images, or provide users with a method to flag images. Further, officials from 4 of the 19 ESPs stated that costs have prevented them from implementing these types of methods, and thus they have relied solely on user complaints to detect apparent child pornography.
- **Technology:** Officials with whom we spoke from 10 of the 19 ESPs had concerns related to technology in reporting and detecting apparent online

³³Pub. L. No. 110-401, § 501(a) (codified at 18 U.S.C. § 2258A(a)(1),(f)).

³⁴According to NCMEC officials, there is no way to know how many, or which, ESPs do not report because there is no known source or list of all existing ESPs. Officials also stated that those ESPs that do not report may not have apparent child pornography on their networks to report.

³⁵Officials could report having more than one concern.

child pornography. For example, officials from 5 of these 10 ESPs stated that making a large number of reports, which can contain hundreds of files per report and multiple submissions, can be a slow process if done manually, and officials from 3 of these 5 ESPs also stated that reporting can be technically challenging to automate.

- Psychological Impact: Officials from 10 of the 19 ESPs reported having concerns over their employees' psychological discomfort that sometimes results from exposure to apparent child pornography images.
- Litigation: Officials from 7 of the 19 ESPs reported having concerns about being sued as a result of their reporting responsibilities under the Act. For example, officials from 2 ESPs stated that forwarding apparent child pornography images in fulfillment of their responsibilities under the Act could make them subject to liability for possessing and transmitting such images. However, the Act states that any civil claim or criminal charge against an ESP arising from the performance of reporting or preserving information may not be brought in any federal or state court.³⁶ Another official stated that the ESP is often sued for using methods to detect apparent online child pornography by the customers it reports.

In response to such concerns, in August 2010, NCMEC provided a guide to registered ESPs that contained, among other things, resources ESPs could use to help report to the CyberTipline as well as information on detecting apparent child pornography on their networks.³⁷ For example, NCMEC's guide includes information on how to automate reporting by building an interface between the CyberTipline and an ESP's system so that ESPs can make a large number of reports, such as several hundred, faster. NCMEC also provides information on how ESPs may address the psychological impact on employees when they view apparent online child pornography in order to make reports to the CyberTipline. For example, NCMEC's guide provides two resources for individuals who have been exposed to child pornography during the course of their work. Employees may contact NCMEC to speak to staff in its Safeguard program, and they may access OJJDP's Web site called Supporting Heroes in Mental Health Foundational Training, which provides resources such as videos, guides,

³⁶Pub. L. No. 110-401, § 501(a) (codified at 18 U.S.C. § 2258B(a)). Under the Act, ESPs are required to preserve information reported to the CyberTipline for 90 days. § 2258A(h).

³⁷Prior to developing the guide, NCMEC provided information to ESPs about their legal obligations to report to NCMEC under the Act and, according to NCMEC officials, plans to continue such action. For example, NCMEC officials attended conferences twice a year where they provided ESPs with information about its CyberTipline and answered ESPs' questions. Officials said that NCMEC also answers ESPs' questions about making reports to the CyberTipline through phone calls and e-mails.

and an online forum.³⁸ Related to concerns about liability, the guide includes excerpts from the Act about ESPs' reporting requirements, which state that ESPs have immunity if a lawsuit is brought against them for downloading and transmitting apparent child pornography if it was during the course of fulfilling their reporting duties. NCMEC is providing ESPs with information about their responsibilities to report incidents of apparent online child pornography to the CyberTipline through the guide; however, it is too early to tell whether these concerns have been addressed.³⁹

NCMEC Provides ESPs Voluntary Methods to Help Reduce Apparent Online Child Pornography, and Some ESPs Have Developed Their Own Means to Detect It

Although ESPs are not required to monitor their networks, NCMEC provides registered ESPs with voluntary proactive methods that they may use to detect apparent online child pornography and then report it as the Act requires. These methods include:

- Key word lists: NCMEC provides lists that contain terms often associated with child sexual exploitation.
- Uniform Resource Locator (URL) sharing: NCMEC distributes a daily list of URLs—which specify the address of a Web page and how to retrieve it—containing apparent online child pornography to ESPs. ESPs can use this information to help prevent the distribution of child pornography. For example, ESPs that host Web sites can check the URL list to ensure that none of the sites that they host are on the list.
- Hash value sharing: NCMEC provides a list of hash values of apparent online child pornography to ESPs which use specialized software to detect and remove illegal files from their systems.

In addition, officials to whom we spoke from 9 of the 19 ESPs reported taking their own proactive measures to detect and help reduce apparent online child pornography on their networks so that it may be reported to the CyberTipline. For example, in addition to receiving customer

³⁸The CyberTipline Safeguard Program provides training and consultation to NCMEC staff members exposed to harmful content (i.e., child sexual abuse images). The goal of the program is to minimize potential harm as a result of viewing objectionable material on a daily basis. This goal is accomplished through the use of in-house social workers and regular visits by a consulting, private psychologist. ESPs that express interest in developing their own wellness programs may contact NCMEC to discuss how to develop a similar program for their employees.

³⁹Because the guide was new, we did not solicit ESPs' opinions about it. Instead, we compared the contents of the guide to the concerns ESPs identified to determine the extent to which the guide provided information that could help to address these concerns.

complaints, 4 of these ESPs said that they monitor or moderate chat rooms and forums for apparent online child pornography and 6 reported using key word lists to search for child pornography, while 3 ESPs reported that they use both of these methods. These 9 ESPs reported that they have these additional, proactive mechanisms in place to better detect apparent online child pornography because they do not want to allow such illegal activity on their Web sites. On the other hand, officials from 10 of 19 ESPs reported that they had not implemented their own additional methods. However, 8 of these 10 used NCMEC's URL and hash value sharing initiatives, according to NCMEC. The remaining 2 ESPs did not implement any methods due to cost concerns, and noted that implementing additional methods to detect apparent child pornography would be a business decision that would require them to consider costs, as well as the types of services they provide.

Further, according to three civil liberties organizations we interviewed, consumers want to use the Internet freely and do not want their online activities to be monitored. They stated that ESPs' proactive monitoring also raises potential constitutional issues because if ESPs are acting as agents of the government when they search users' activities and communications, they are subject to the requirements of the Fourth Amendment to obtain probable cause and a search warrant.⁴⁰ However, officials we spoke with from the 9 ESPs that utilize these methods stated that their terms of service specify that users cannot conduct illegal activity while on their networks, which includes the possession or trading of child pornography. Therefore, they said that methods to detect apparent child pornography are a means of ensuring compliance with the ESPs' terms of service, which is distinct from conducting government-directed searches for information.

⁴⁰*See, e.g., U.S. v. Richardson*, 607 F.3d 357 (4th Cir. 2010) (holding that AOL was not acting as a government agent subject to the requirements of the Fourth Amendment when it searched defendant's e-mail and subsequently reported child pornography it found to NCMEC in conformance with requirements now codified at 18 U.S.C. § 2258A).

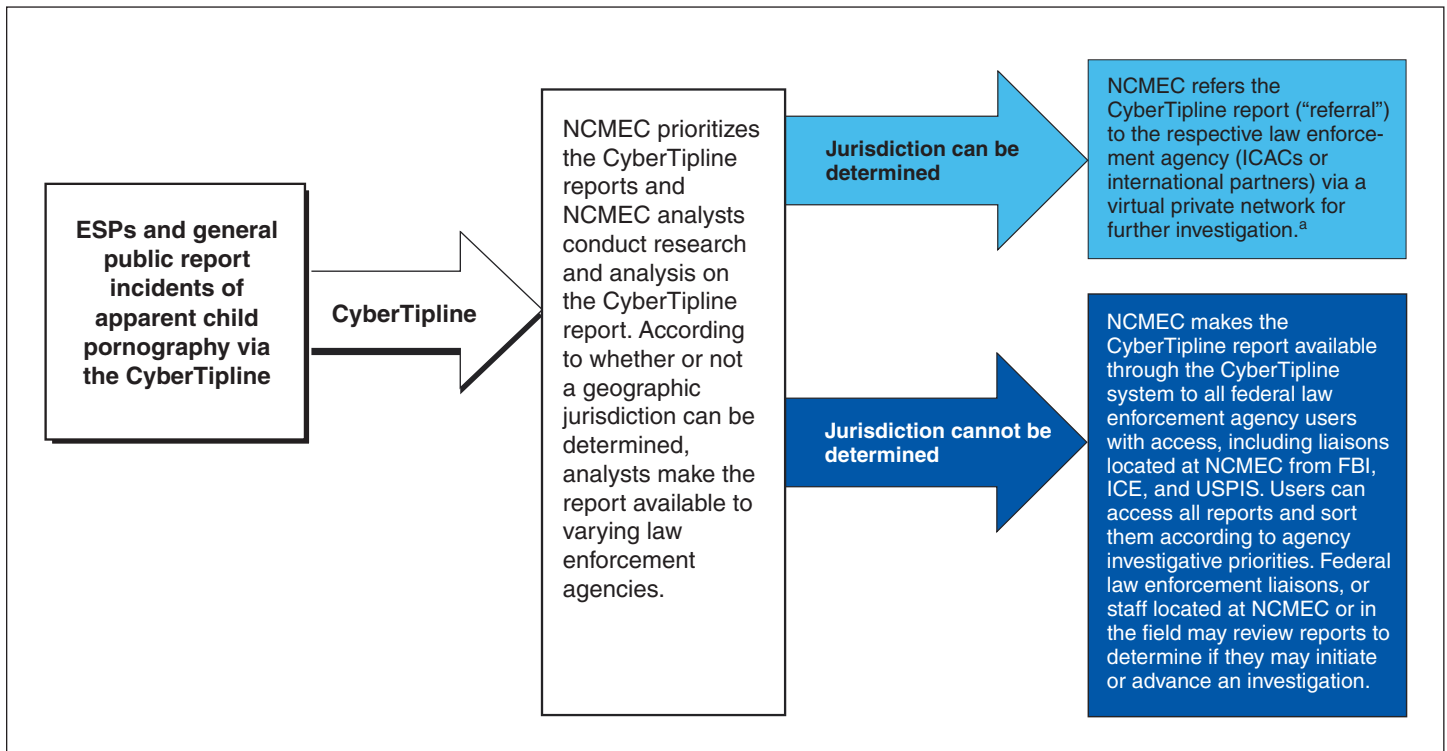
**Expanding Feedback
from Law
Enforcement Could
Help Improve the
Usefulness of
CyberTipline Reports
and Better Address
Increasing Number of
Reports**

**NCMEC Makes
CyberTipline Reports
Available to Law
Enforcement Based on
Jurisdiction**

As required under the Missing Children's Assistance Act, NCMEC refers CyberTipline reports of apparent child pornography from ESPs and the general public to federal, state, local, and international law enforcement agencies for investigation, as shown in figure 2.⁴¹

⁴¹42 U.S.C. § 5773(b)(1)(P).

Figure 2: Overview of NCMEC Process for Receiving and Disseminating CyberTipline Reports



Source: GAO analysis of NCMEC; FBI; ICE; and USFIS data.

^aVirtual private networks allow NCMEC to disseminate CyberTipline reports to ICAC task forces or international partners through secure encrypted connections.

When a CyberTipline report is initially submitted by an ESP⁴² or the general public, the reporting party must select one of eight “reporting categories,” including possession, manufacture, and distribution of child pornography.⁴³ NCMEC then prioritizes the CyberTipline reports and

⁴²The PROTECT Our Children Act of 2008 requires ESPs to report any facts and circumstances from which there is an apparent child pornography violation. However, the facts and circumstances that an ESP possesses or includes in its report may vary.

⁴³The other seven reporting categories are: online enticement of children for sexual acts, child prostitution, sex tourism involving children, extrafamilial child sexual molestation, unsolicited obscene material sent to a child, misleading domain names, and misleading words or digital images on the Internet.

analysts conduct research and analysis on them.⁴⁴ This analysis may include: (1) determining whether an alleged child pornography image is that of an actual child; (2) determining whether an image in a CyberTipline report is new or has been viewed by law enforcement in the past, which may indicate whether the child in the image is currently being abused; or (3) among other things, reviewing e-mail addresses, Web addresses, and other information to determine if the offender associated with the CyberTipline report may be involved in an organized child pornography sharing ring. After processing the CyberTipline report, NCMEC analysts select a “reclassified incident type” which best describes the completed CyberTipline report. There are currently 17 reclassified incident types, including confirmed child pornography.⁴⁵ NCMEC officials stated that once a CyberTipline report and any associated analysis has been reclassified, it does not necessarily mean the tip will be useful to law enforcement in initiating or advancing an investigation. The determination as to whether a CyberTipline report may be useful in initiating an investigation is at the judgment of law enforcement personnel.

NCMEC analysts make the CyberTipline report and their analysis available to law enforcement according to whether or not a geographic jurisdiction can be determined. When the geographic jurisdiction of a CyberTipline report can be determined based on the location of the suspect, the victim, or both,⁴⁶ NCMEC will refer the report (“referral”) to the respective law enforcement agency (primarily ICAC task forces) via a secured system called a virtual private network.⁴⁷ However, when the jurisdiction of a

⁴⁴NCMEC assigns a priority level to every CyberTipline report received. CyberTipline reports that indicate a child is in imminent danger, such as online enticement, are priority 1. Reports of child pornography from registered ESPs that are made to the registered ESP reporting Web page are designated priority 4. This priority level indicates that the report may contain illegal content.

⁴⁵The other 16 reclassified incident types are: child pornography (not Internet-related); child pornography (unconfirmed); child pornography (unconfirmed – international); child prostitution; child sex tourism; child sexual molestation; child trafficking (nonsexual exploitation); cyberbullying; online enticement – pretravel; online enticement – travel; other type of incident; appears adult; not enough info/dummy record; SPAM; unable to access; and ESP test report.

⁴⁶Jurisdictional information may include address, zip codes, IP addresses, state, or cell phone numbers. According to NCMEC officials, analysts conduct open-source, online searches in an attempt to determine possible jurisdiction or corroborate information in the initial CyberTipline report.

⁴⁷Virtual private networks allow NCMEC to disseminate CyberTipline reports to ICAC task forces through secure encrypted connections.

CyberTipline report cannot be determined because, for example, the ESP did not include a zip code or IP address, NCMEC makes the report available through the secure CyberTipline system to federal law enforcement agency users who have access to the system.⁴⁸ As of November 24, 2010, 41 federal law enforcement users had access to this secure system, including agency liaisons from FBI, ICE, and USPIS who are located at NCMEC.

The CyberTipline system allows users to access all CyberTipline reports ever submitted, as well as search for and prioritize reports of specific reclassified incident types that are of investigative interest to the agency. According to NCMEC officials, the search function was designed at the federal agencies' request to allow them streamlined access to those reports which, based on reclassified incident types, they indicated most often fall within their investigative purview. For example, the FBI liaison can choose to search for all CyberTipline reports associated with confirmed child pornography. Federal law enforcement liaisons, or staff located at NCMEC or in the field, may review reports to determine if they may initiate or advance an investigation, as described in table 2.

Table 2: Overview of Process Different Federal Agencies with Liaisons at NCMEC Use to Review and Forward CyberTipline Reports for Investigation

Agency	Overview of CyberTipline report review
FBI	To address CyberTipline reports and child pornography, FBI has one liaison assigned to NCMEC who supervises two Investigative Support Specialists who review the reports. FBI officials stated that they prioritize child pornography-related CyberTipline reports based on, among other things, whether they fall within their investigative purview and whether or not a jurisdiction or subject can be determined. However, among the reports that meet those parameters, officials said that they are not able to further prioritize the reports until they open them and can determine what type of information is included in the report. When FBI Investigative Support Specialists determine that a CyberTipline report is likely to enable the agency to initiate or advance an investigation, they prepare an investigative packet, for which they supplement information from the report (or numerous other reports), with FBI data as well as data from other sources. They then submit the packet to the FBI liaison who reviews it and forwards it to FBI field agents for investigation.

⁴⁸Federal law enforcement has the authority to obtain jurisdictional information through the legal process, such as by serving a subpoena. Therefore, according to NCMEC officials, federal law enforcement liaisons are the appropriate recipients of CyberTipline reports in which no jurisdiction was determined by NCMEC because they are sometimes able to determine a jurisdiction based on other information in the report when they serve a subpoena to an ESP to obtain the suspect's location because they can use such legal process to obtain additional information.

Agency	Overview of CyberTipline report review
ICE	According to ICE officials, while ICE can access and review CyberTipline reports in the CyberTipline system, most CyberTipline reports reviewed by ICE officials are sent directly to them via e-mail from NCMEC analysts. In addition, according to officials, ICE uses its resources to assist NCMEC in disseminating CyberTipline referrals to foreign law enforcement agencies. ICE has established virtual private network connections in approximately 10 countries, allowing the dissemination of CyberTipline referrals to the responsible law enforcement agencies in these countries.
USPIS	Currently, the USPIS liaison located at NCMEC does not review CyberTipline reports; rather up to five field postal inspectors with subject matter expertise have access to the CyberTipline system and review the reports. According to the Child Pornography National Program Manager for USPIS, NCMEC also e-mails CyberTipline reports determined by NCMEC analysts to have a nexus to the mail directly to the USPIS liaison located at NCMEC. The liaison then sends any CyberTipline report that has a solid U.S. mail nexus to the field for attention. The official said that the agency focuses on CyberTipline reports that have (1) a viable nexus to U.S. mail, (2) a viable mailing address, and (3) cooperation of the victim and/or the reporting party (e.g., parent or guardian). The official added that a new liaison would be assigned to NCMEC in the spring of 2011 and that this individual would review CyberTipline reports.

Source: FBI, ICE, and USPIS.

The CyberTipline provides leads for federal, state, and local law enforcement agencies, along with their own sources, such as undercover investigations. For example, according to FBI officials, the FBI develops approximately 100 to 200 investigative leads per year to be used to initiate investigations based on CyberTipline reports, and a USPIS official estimated that about 10 percent of leads come from the CyberTipline. Officials we interviewed from seven of the eight task forces stated that CyberTipline reports make up 50 percent or more of their leads, and five of those seven reported receiving between 80 to 95 percent of their leads from CyberTipline reports.⁴⁹

Soliciting Additional Information on the Usefulness of CyberTipline Reports Could Help NCMEC Ensure Reports Are as Useful as Possible to Law Enforcement

The number of CyberTipline reports NCMEC received and made available to law enforcement agencies has increased over the past few years, making it important that these reports are as useful as possible to the law enforcement agencies investigating online child pornography. According to NCMEC, the number of CyberTipline reports determined by federal law enforcement agencies to be most often within their investigative purview has increased by about 134 percent from about 74,000 in 2008 to about 173,000 in 2010. Similarly, the number of CyberTipline reports that

⁴⁹An official from the eighth task force stated that the ICAC received about 10 to 15 percent of its leads from the CyberTipline but generally relied on undercover investigations for its leads.

NCMEC referred to ICAC task forces increased about 71 percent from about 14,000 in 2008 to about 24,000 in 2010.⁵⁰

However, according to the FBI liaison at NCMEC and officials in six out of eight ICAC task forces we contacted, information in individual CyberTipline reports was not always useful for initiating law enforcement action, such as obtaining a subpoena, initiating an investigation, or executing a search warrant.⁵¹ For example, according to these officials, reports initially submitted to NCMEC by the ESP or the general public may:

- not contain information, such as an IP address or an image;
- contain old data provided by ESPs, which may prohibit obtaining a subpoena;
- contain an image that did not meet the legal definition of child pornography; or
- include information that is not a violation of child pornography laws in general or in a particular state.

NCMEC makes these CyberTipline reports that do not contain certain information, such as an IP address or image, available to law enforcement because, according to NCMEC officials, it believes that law enforcement may be able to use other information in the report to further other investigations. For example, according to these officials, a CyberTipline report may have an e-mail address or username that is associated with a known offender, and the information in it may be useful to an ongoing law enforcement investigation. Federal law enforcement officials from FBI, ICE, and USPIS who work directly with NCMEC, as well as officials in five of the eight ICAC task forces, stated that receiving such reports could be useful, for example, to furthering other ongoing or future investigations.

NCMEC takes steps to obtain feedback on the usefulness of CyberTipline reports made available to law enforcement. Specifically, NCMEC solicits feedback via e-mail or in person each quarter from the federal law enforcement liaisons at NCMEC about the usefulness of the CyberTipline

⁵⁰The number of reports provided by NCMEC to law enforcement agencies does not equate to the actual number of incidents of apparent child pornography being reported because, for example, different individuals may have reported the same incident to an ESP and each of these reports is recorded separately.

⁵¹Officials from one ICAC task force stated that they found all information valuable and officials from one ICAC task force did not provide information on usefulness.

reports overall. According to NCMEC officials, the questions they pose vary and are intended to obtain a general idea of the usefulness of the CyberTipline reports. Officials from FBI and USPIS who work directly with NCMEC in reviewing CyberTipline reports confirmed that they speak to NCMEC officials on a continuous basis to discuss the status of CyberTipline reports that they have taken action on and their outcomes, as well as how the process of providing reports could be improved. For ICAC task forces, NCMEC sends a feedback form approximately 8 weeks after referring a CyberTipline report that includes a question asking whether or not the information provided by NCMEC's analysts in the CyberTipline report was useful.⁵²

However, NCMEC does not systematically collect information on how useful individual reports are to initiating and advancing investigations from law enforcement users or the extent to which reports contain specific types of information law enforcement may need. For example, NCMEC does not have a systematic process—a standard set of questions applied consistently over time—for obtaining information from federal liaisons about why individual CyberTipline reports may or may not be useful in initiating or advancing investigations and what the information gaps are that limited their usefulness. Similarly, NCMEC does not ask ICAC task forces why individual CyberTipline reports were or were not useful and how they could be made more useful. Capturing this type of feedback could help NCMEC work with law enforcement to determine which reports do not assist in initiating and advancing investigations, why not, what key information is missing, whether NCMEC could add more analysis to supplement reports, and what steps it might take to assist ESPs in including as much useful information as possible in future CyberTipline reports. In addition officials in six of the eight ICAC task forces we selected reported that such an assessment of which elements make a CyberTipline report more useful could enhance law enforcement's ability to use the information to further investigations. For example, one commander noted that such an assessment would be helpful in providing a more focused report for investigative follow-up.

Soliciting such information about the usefulness of CyberTipline reports is consistent with best practices, such as regularly soliciting stakeholder input and involving stakeholders early and throughout the decision-making process that we have previously reported for effectively meeting

⁵²This form also contains five other questions related to case status.

stakeholder needs.⁵³ Further, we have reported that by comprehensively soliciting feedback from all of its users, an agency can better ensure that it has a full picture of the needs of those users and how well it is meeting those needs, and can also make improvements that are relevant to them.⁵⁴ NCMEC officials acknowledged that they would like to obtain more feedback from law enforcement agencies and could explore more targeted ways of obtaining it. For instance, during our meetings with NCMEC officials, these officials discussed ways to facilitate the better collection of feedback, such as creating a systematic process for obtaining feedback from the federal agencies; adding additional questions geared toward understanding why an individual CyberTipline report was or was not useful; developing an easier-to-use electronic feedback form; or holding ongoing discussions with ICAC commanders on how the process of collecting feedback can be improved. However, NCMEC officials said that they did not yet have plans in place for implementing such feedback mechanisms in part because they do not want to overburden law enforcement agencies. Our interviews with law enforcement agencies indicate that these agencies see benefit in having this feedback. Taking steps to work with law enforcement to determine effective ways to enhance its feedback processes could help NCMEC better ensure that law enforcement receives the most useful information to initiate and advance investigations and could also help NCMEC provide more focused guidance to ESPs in terms of what types of information to include in CyberTipline reports.

⁵³GAO, *Anti-Money Laundering: Improved Communication Could Enhance the Support FinCEN provides to Law Enforcement*, [GAO-10-141](#) (Washington, D.C.: Dec. 14, 2009); GAO, *Juvenile Justice: DOJ is Enhancing Information on Effective Programs, but Could Better Assess the Utility of This Information*, [GAO-10-125](#) (Washington, D.C., December 2009); *Performance Budgeting: PART Focuses Attention on Program Performance, but More Can Be Done to Engage Congress*, [GAO-06-28](#) (Washington, D.C., October 2005); *Transportation Research: Opportunities for Improving the Oversight of DOT's Research Programs and User Satisfaction with Transportation Statistics*, [GAO-06-917](#) (Washington, D.C.: Aug.15, 2006).

⁵⁴[GAO-06-917](#).

Existing Deconfliction Mechanisms, While Fragmented, Generally Prevent Pursuit of the Same Suspects; DOJ Is Starting to Develop a National System

Deconfliction Mechanisms Vary but Generally Help to Avoid Duplication of Effort

In 22 of 28 interviews we conducted with cognizant supervisory special agents from FBI, ICE, and USSS; postal inspectors; and ICAC task force commanders in the judicial districts we visited, law enforcement officials reported that they concurrently used various automated and nonautomated deconfliction mechanisms to help resolve conflicts in online child exploitation investigations and prevent pursuit of the same suspects.⁵⁵ Nonautomated procedures include: the use of interpersonal relationships or contacts between investigators from different law enforcement entities or task forces to resolve case conflicts; deconfliction reports and services that NCMEC provides to ICAC task forces and federal law enforcement agency personnel; and exchanges of law enforcement information through area Project Safe Childhood coordinators.⁵⁶ For example, an ICE Assistant Special Agent in Charge (ASAC) we interviewed reported that deconfliction is often accomplished through interaction between agents from the different agencies investigating the case. The agency with the best evidence generally conducts the investigation, in some instances with assistance from other law enforcement agencies.

In instances where law enforcement agencies determine through these mechanisms that they are pursuing the same target, officials said that an option is for one agency to discontinue its investigation and allow another agency to pursue the target instead. The agencies involved can compare

⁵⁵In 6 of the 28 interviews, officials indicated that they had not pursued the same target as another agency.

⁵⁶NCMEC produces a monthly deconfliction report that provides information on the status of CyberTipline reports referred to ICAC task forces. FBI, ICE and USPIS liaisons located at NCMEC provide information and research to investigators in the field.

the evidence each one has collected as well as the focus of their investigations before determining which agency is in the best position to proceed with the investigation. These officials also said that deconfliction is important because there is potential for inefficiencies and waste of investigative resources when multiple agencies are pursuing the same target. For example, an FBI Supervisory Special Agent cited an instance when the agency learned that a local law enforcement agency had already made contact with a suspect a month before the FBI served a search warrant. Not all duplication is inefficient, however, as there are instances where multiple agencies pursue the same target for different offenses. For example, one agency may be investigating the target as a suspect for distribution of child pornography and another investigating the target for sexual abuse. Nevertheless, in 22 of 28 interviews, officials said that they are able to resolve most case conflicts by using a combination of nonautomated and automated deconfliction mechanisms.

Officials in 14 of the 28 interviews also reported using automated investigative systems to identify information and track suspects engaging in trafficking child pornography online.⁵⁷ These investigative systems covertly identify and monitor computer networks where users share files directly with one another, also known as peer-to-peer file sharing.⁵⁸ These covert investigative systems also provide deconfliction for investigators allowing registered users to share case information and avoid initiating duplicate investigations on targets already under investigation. In 12 of 28 interviews, law enforcement officials also reported avoiding pursuing the same child pornography targets by checking information about a suspect against external law enforcement databases, such as the SafetyNet system in New York, and systems containing national crime data, including the National Crime Information Center.⁵⁹ These databases can be used to

⁵⁷Because we asked officials about deconfliction mechanisms and other efforts in place to avoid duplication of effort among law enforcement agencies in general, not all officials provided information on the use of specific types of deconfliction mechanisms.

⁵⁸Peer-to-peer file sharing programs are Internet applications operating over peer-to-peer networks that enable direct communication between users.

⁵⁹SafetyNet is an integrated records management system for law enforcement agencies that provides reporting and analysis capabilities to assist with crime prevention, investigation, and incident analysis. The National Crime Information Center is a computerized index of criminal justice information maintained by the FBI and made available to federal, state, and local law enforcement and other criminal justice agencies nationwide. Its files contain among other items, criminal record history information and information on fugitives, stolen property, and missing persons.

ascertain whether a target has a criminal history or is also under investigation by other law enforcement entities, among other things.

However, law enforcement officials in 7 of 28 interviews, as well as two senior DOJ officials, reported limitations with the existing automated investigative systems and law enforcement databases that can impact their usefulness in child pornography investigations. Among the limitations, these officials stated that an automated system or database does not exist that provides comprehensive case information and deconfliction for all federal, state, and local law enforcement agencies. Since a comprehensive deconfliction system for all law enforcement entities is not yet available, the automated systems in use provide investigators with partial case information because, in general, these systems and databases are not integrated. For example, the investigative systems do not integrate information, in part, because the systems are developed by different organizations, and the developers limit access to case information to registered users of their systems in order to control who has access to investigative information. These officials also reported that another factor that contributes to the absence of a comprehensive national system for deconfliction are prohibitions by federal and state agencies which restrict access to investigative information by external law enforcement entities. For example, according to DOJ, the FBI always must consider case and security concerns when sharing information. In addition, a DOJ Deputy Associate Administrator said that federal agencies have requirements to use their own data systems, which often allow limited or no external access to other entities. DOJ officials also agreed that because of the partial or fragmented information, the available automated systems may contribute to information sharing obstacles between agencies and difficulties in coordinating actions between investigations. These officials agreed further that this can also impede compilation of strategic information on the most dangerous offenders and adversely impact identifying new trends that offenders are using online to attempt to exploit children. DOJ is beginning to develop a national system to address some of these shortcomings, as we discuss in the following section.

DOJ Is in the Early Stage of Developing a National System to Provide a Deconfliction Tool

The Act requires the Attorney General to develop a National Internet Crimes Against Children Data System (NIDS), an online data system that is to include information-sharing capacity, case deconfliction, and other capabilities. According to the Act, the purpose and intent of NIDS, among other things, is to create a deconfliction system for ICAC task forces, as well as for federal, state, local, and tribal law enforcement agencies that investigate and prosecute child exploitation crimes. The planned

deconfliction component is to allow authorized law enforcement agencies to access NIDS and contribute information to resolve conflicts in online child pornography investigations. DOJ officials overseeing the development of NIDS reported that NIDS is intended to address the known deconfliction limitations of existing investigative systems, such as reporting partial or fragmented case information, as well as the lack of data sharing among various law enforcement entities due to system integration. The officials stated that NIDS is also to incorporate new and emerging technologies, rather than being based solely on existing investigative systems. Appendix III provides a description of NIDS functions required by the Act.

The Act does not specify a time frame for NIDS implementation, but according to senior DOJ officials, issuance of the solicitation for the development of NIDS was delayed until spring 2010 because the National Coordinator had not been selected, funding was not sufficient to construct the NIDS system, and the complexity of the system made it difficult to develop and implement. More specifically:

- DOJ issued the initial solicitation for the construction, maintenance, and housing of NIDS in March 2009, 9 months before it selected a National Coordinator. Once a National Coordinator was appointed in January 2010, DOJ decided to issue a revised solicitation to, among other things, conduct a needs assessment to collect requirements information for the future development of NIDS. DOJ issued this revised solicitation in June 2010. Generally accepted information technology system development practices call for organizations to follow a disciplined approach, including performing a needs assessment to define system requirements prior to beginning system acquisition activities.⁶⁰ As described later, this information is to serve as an assessment of technical requirements for the construction of NIDS, and DOJ plans to use the requirements as the basis to determine how to build NIDS.
- The National Coordinator reported that funding was not appropriated to support development of a system as complex as NIDS. The Act authorizes \$2 million for NIDS in each of fiscal years 2009 through 2016. However, DOJ officials stated that the agency did not request funds for NIDS in the fiscal year 2012 President's Budget because American Recovery and Reinvestment Act of 2009 (ARRA) funding was available beginning in 2009

⁶⁰GAO, *Information Technology, Opportunities Exist to Improve Management of DOD's Electronic Health Records Initiative*, GAO-11-50, (Washington D.C.: October 2010), 25.

and extending to the end of fiscal year 2010.⁶¹ DOJ is funding the NIDS needs assessment project through an ARRA grant it awarded to the ICAC task forces, which provided about \$921,000 and was obligated in fiscal year 2010 and is to run through fiscal year 2011. DOJ officials noted that the department has not yet developed a projection of the cost to construct and implement NIDS because it must first determine the technical requirements for NIDS.

- The National Coordinator also reported significant challenges associated with the development of NIDS. Among these challenges, the Act requires NIDS to incorporate a method for law enforcement to conduct covert investigations of child pornography suspects online and provide for a case deconfliction system, as well as gather and analyze child pornography related data, among other things. In addition, the National Coordinator said that DOJ must ensure NIDS is accessible by ICAC task forces, and federal, state, local, and tribal law enforcement agencies, which presents a challenge because the systems these entities use may not be compatible. The National Coordinator reported that a system with the intended capacity of NIDS will be a challenge to construct; however, DOJ officials believe it can be accomplished and stated that an interim step in the process of constructing it will be the development of the needs assessment to determine NIDS requirements.

In general, the 2010 NIDS needs assessment grant solicitation is for evaluating case deconfliction and covert investigative capabilities of existing software and investigative tools. The solicitation is also for determining the information reporting capabilities among federal, state, and local law enforcement agencies to assist in identification of offenders; identifying the shortcomings in these agencies' systems and developing new software and investigative tools that address these identified shortcomings; assisting law enforcement agencies in covert investigations; and supporting research to identify and predict which offenders are most dangerous so that DOJ can use that information to identify high-priority suspects to timely report them to law enforcement agencies.

In September 2010, after conducting a competitive solicitation for proposals and an external peer review process for the NIDS proposal, DOJ selected an existing ICAC task force agency, the Massachusetts State

⁶¹Pub. L. No. 111-5, 123 Stat. 115, 130 (2009). ARRA provides DOJ with funding for grants to assist state, local, and tribal law enforcement to combat Internet crimes against children, among other things. ARRA funding was available for obligation until the end of fiscal year 2010.

Police, as the grantee.⁶² The grant recipient, along with the Pennsylvania ICAC task force and the University of Massachusetts Amherst, previously developed an investigative system which is currently in use by 58 of 61 ICAC task forces nationwide.⁶³ Because of this experience, expertise reflected in the proposal submitted, and the recommendations of the external peer reviewers, DOJ determined this grant recipient would be qualified to complete the needs assessment and other activities as required by the 2010 NIDS solicitation.

In October 2010, DOJ initiated the effort to conduct a needs assessment to identify NIDS requirements and plans to complete the effort within 12 to 24 months. Until this initial work is done, however, DOJ will not know precisely when NIDS is to become operational. Therefore, the national deconfliction system the Act requires may not be operational for a number of years. In the meantime, however, DOJ has approved the continued use of existing automated systems for case deconfliction purposes as a stopgap measure.

Backlogs in Forensic Analysis of Digital Evidence and Length of Time ESPs Retain User Data Can Hinder Investigations

Assessing the Costs and Benefits of Forensic Analysis Steps Could Help Determine Efficiencies to Reduce Backlogs

According to prosecutors in DOJ's CEOS, the information contained on a suspect's hard drive is key to an investigation of online child pornography, and the forensic analysis of suspects' computers is the most important aspect of an investigation of this crime. Forensic analysis of digital evidence includes the extraction and review of information from digital media, such as computer hard drives, and can prove possession, receipt,

⁶²The Massachusetts State Police partnered with Fox Valley Technical College, University of Massachusetts, and University of New Hampshire Crimes Against Children Research Center.

⁶³The ICAC task forces use multiple investigative tools.

distribution, or production of online child pornography.⁶⁴ However, headquarters officials we interviewed responsible for overseeing forensic analysis to address child pornography crimes from FBI, CEOS, ICE, USSS, and USPIS all reported that forensic resources available to review digital evidence in support of investigations and prosecutions of online child pornography crime are scarce relative to the demand for such services. Further, they all stated that backlogs in the forensic analysis of suspects' computers to extract and analyze evidence, such as images or chat logs, may delay and, in some cases, hinder investigations and prosecutions of offenders.⁶⁵

According to a 2007 FBI memorandum, subjects of a child pornography investigation are usually not arrested when a suspect's computer is seized, but after full forensic examination is completed, which, according to DOJ officials, may take a period of 1 week to over 1 year in some cases, depending on the level of detailed forensic analysis requested by prosecutors or investigators, or because of the needs of the individual case. However, ICE and FBI agents we interviewed who investigate these crimes stated that if there is a perceived imminent threat from the suspect, such as evidence that a child is being abused, the suspect may be arrested immediately or forensic analysis of the suspect's computer may be expedited to facilitate faster arrest. FBI's 2007 memorandum also expressed a concern that delays in charging suspects while forensic examinations take place could allow potential abusers of children to remain free to commit additional crimes until digital evidence had been examined, and it is determined there is enough evidence to arrest and indict the suspect. The memorandum went on to state that it is possible that this scenario can lead to increased exposure of children to child

⁶⁴Forensic analysis of digital evidence can be conducted on different types of media, such as global positioning system devices, memory cards, or compact discs, and can be conducted by federal, state, and local law enforcement agencies in support of a variety of investigations, such as online child pornography crime and identity theft.

⁶⁵Currently, no governmentwide standards or criteria exist for federal law enforcement for how to calculate the timeliness of forensic analysis or backlogs in analysis, and various law enforcement agencies have developed their own measures to calculate and track timeliness and backlogs. For example, the FBI categorizes a request for forensic examination of digital evidence as being in backlog status if: (1) after being submitted for examination, more than 30 days have passed without a lead examiner being assigned, or (2) a request has been assigned to an examiner and more than 60 days have passed without the examination being completed. ICE defines a request for forensic analysis as being in backlog if action is not taken on digital media upon arrival. For the purposes of this report, the term backlog refers, in general, to any delay in forensic analysis.

predators. Similarly, the National Academy of Sciences⁶⁶ reported in a 2009 review of forensic practices that backlogs in any area of forensic analysis, including analysis of digital evidence, can contribute to the release of guilty suspects who go on to commit further crime, as well as result in delayed investigations of those who are not yet charged.⁶⁷

DOJ headquarters prosecutors stated that no comprehensive statistics exist as to whether or to what extent suspects have continued to engage in child pornography crime while their computers are analyzed. However, federal law enforcement officials we interviewed who investigate these crimes stated that suspects have, in some instances, continued to commit crimes. For example:

- ICE officials in Kansas City stated that after being served a search warrant, one suspect purchased a new computer and continued to engage in the receipt of online child pornography.
- ICE Cyber Crimes Center officials stated that after one California suspect's computer was seized, he purchased a new computer and warned individuals with whom he had been trading child pornography images that an investigation was taking place.

Several Factors May Contribute to Backlogs in Forensic Analysis of Digital Evidence

Headquarters officials from FBI, ICE, CEOS, USFIS, and USSS that we interviewed who oversee forensic analysis all identified several factors that may contribute to backlogs in forensic analysis. These include the increase in the volume of people using computers and the Internet, the low cost and ease of obtaining digital media storage capacity, and the wide variety and constant evolution of technologies being used by offenders. For example, FBI statistics show that the volume of data processed at its Regional Computer Forensic Laboratories⁶⁸ has increased almost 3,000

⁶⁶The National Academy of Sciences is a federally sponsored entity chartered to investigate, examine, experiment, and report on any subject of science and provide advice on the scientific and technological issues that pervade policy decisions.

⁶⁷The report also stated that backlogs in forensic analysis can result in prolonged incarceration for innocent persons wrongly charged and awaiting trial. National Research Council of the National Academies. "Strengthening Forensic Science in the United States, a Path Forward." (The National Academy Press, Washington, D.C.: 2009).

⁶⁸The FBI has partnered with other federal, state, and local law enforcement agencies to establish 14 Regional Computer Forensic Laboratories to examine digital evidence in support of criminal investigations in areas such as child pornography, terrorism, financial crimes, and fraud. According to FBI officials, 2 additional laboratories in Los Angeles and New Mexico are to begin operations in 2011. These laboratories are staffed by federal, state, and local law enforcement agency personnel who are trained and certified by the FBI to collect and examine digital evidence pursuant to FBI requirements.

percent, from approximately 82 terabytes in fiscal year 2003 to 2,334 terabytes in fiscal year 2009.⁶⁹

In addition, variations in the amount of digital evidence federal prosecutors request to be reviewed in support of prosecutions of online child pornography crimes may increase the amount of time needed for forensic analysis of digital evidence and further contribute to backlogs. For example, two senior officials from FBI's Digital Evidence Section stated that requests by some federal prosecutors that all digital information be reviewed for a given prosecution can increase the amount of time needed at FBI labs for each examination, which further contributes to backlogs at these labs. According to these officials, hard drives and other digital media obtained during investigations could contain hundreds of thousands of images and movies of child pornography, and to review all of them for a single investigation could take a forensic examiner or investigator several months, which may not be efficient.

Alternatively, these FBI officials also stated that a strategy that calls for more thorough reviews of digital evidence for those cases where the suspect's characteristics indicate that the person may pose a physical danger to children would more efficiently allocate scarce forensic resources.⁷⁰ This, in turn, could allow those resources to be used to conduct forensic analysis on a greater number of suspects, which could increase DOJ's ability to prosecute a greater number of offenders. However, prosecutors we interviewed in DOJ headquarters noted that thorough reviews of suspects' digital media can be important because images and movies on that digital media may contain evidence that a child is currently being abused by the suspect. If not all information is reviewed, prosecutors may not be able to prosecute the offender on all charges for which the person is guilty, and all children who are currently being abused may not be identified.

⁶⁹According to FBI officials, this increase is due to increasing amounts of data related to several types of crimes, including fraud and identity theft, as well as online child pornography crime. However, they added that online child pornography and other child exploitation matters take up about 40 percent of the FBI's digital forensics examination, and may constitute a higher percentage at some Regional Computer Forensic Laboratories.

⁷⁰The officials stated, for example, that if an online child pornography suspect were a teacher or was on the sex offender registry, a thorough review of all of the material on that suspect's computer would be called for because the individual would routinely have access to children or may have already abused children. Alternatively, these FBI officials stated, reviews of hard drives belonging to suspects with no access to children and no previous history of child exploitation crime might not need as full a review.

In addition, senior DOJ officials we interviewed stated that a “tiered” strategy that makes more use of forensic review of a suspect’s computer in his or her residence may allow for efficiencies in the forensic process. For example, according to FBI and ICE agents we interviewed who investigate these crimes, reviewing a suspect’s computer within their residence allows law enforcement officers to remove only those computers that are most likely to contain child pornography, which can reduce the number of computers that must be analyzed as well as make it more likely that a suspect confesses. According to prosecutors in DOJ headquarters, increased use of on-scene forensic review of suspects’ computers may also, in some cases, negate the need to send a suspect’s computer to a forensic examiner for review. All of these factors may, in turn, reduce backlogs in forensic analysis. Senior DOJ officials noted that these types of case-by-case decisions are currently being made in the field based on, among other things, the resources available to conduct forensic analysis within the judicial district and the priorities of the U.S. Attorney’s Office.

Another factor that FBI, CEOS, USPIS, and USSS headquarters officials we interviewed who oversee forensic analysis all stated increases backlogs is the steps federal law enforcement agencies take to ensure the integrity of analysis conducted by forensic examiners, which add to the time necessary to complete examinations. According to all of these law enforcement officials, finding apparent child pornography or other evidence on a suspect’s digital media can be done by, among other things, conducting key word searches or opening digital folders on the suspect’s hard drive to review individual images or movies. Steps taken to ensure the integrity of these activities—such as making exact copies of digital evidence on which to conduct any analysis and taking hash values of original evidence before examinations are conducted—are meant to provide a level of assurance that evidence is not tampered with and that examinations can withstand legal challenges in court.⁷¹ However all of these officials stated that these steps may add several hours to several weeks to the laboratory examinations of digital evidence, especially for large volumes of data, and add to the time that subsequent requests for analysis must wait in the queue, which further contributes to backlogs. For example, making an exact copy of a suspect’s hard drive may take several

⁷¹ Any alternation of these electronic files changes the values. Once digital forensic analysis is completed, verifying that the digital fingerprint of the copied evidence still matches that of the original digital evidence mathematically demonstrates that the evidence has not been altered during the process.

days and must be completed before analysis of the information on the hard drive takes place.⁷²

The FBI, through its Computer Analysis Response Team program, takes additional steps to further ensure the integrity of its examination system.⁷³ These steps include:

- Requiring uniform training, certification testing, annual proficiency testing and annual continuing education for all certified FBI digital evidence forensic examiners.
- Documenting all examination processes, including search and review activities undertaken by the forensic examiner, so that they can be duplicated by another examiner, if necessary, to ensure accountability and accuracy.
- Adhering to written forensic protocols which inform the actions of forensic examiners and which are subject to review and audited for compliance.
- Separating the forensic examination and investigative search portions of the forensic review. Forensic examiners typically authenticate and extract subsets of data, such as images or chat logs, from seized digital media which has first been reviewed and searched by investigators. FBI agents then conduct content analysis of these data after examiners extract and deliver them to identify information relevant to a specific investigation.
- Conducting peer reviews of forensic examination reports.

Officials from FBI's Digital Evidence Section stated that these additional steps, while increasing the amount of time necessary to conduct analysis, help to refute any potential claims that there exists a bias on the part of the examiner that influenced the results of a forensic examination. Specifically, the officials stated that these measures are designed to mitigate against the risk that untrained or unqualified forensic examiners could alter digital evidence, which could lead to innocent individuals being

⁷²DOJ officials noted that many agencies conduct on-scene forensics, but do so only after applying a "write-blocker," which is a software tool that allows forensic analysts to examine a suspect's computer hard drives or other digital media without altering data on that media to ensure that data are not added to the suspect's storage media. The "write-blocker" is another step taken to ensure the integrity of the forensic analysis.

⁷³The Computer Analysis Response Team, as well as the Regional Computer Forensic Laboratories, provides assistance to FBI field offices in the search and seizure of computer evidence, as well as forensic examinations and technical support for FBI investigations.

sent to prison. Further, the officials said that initiating these additional steps ensures a degree of separation between agents—who conduct an investigation—and examiners—whose primary function is to carry out specific examination activities prescribed by the agents—and is a means of ensuring that investigative bias cannot easily be introduced in the digital forensic analysis process, particularly with respect to forensic expert opinion analysis relating to questions of how, when, why, and by whom data were created, modified, destroyed, or altered.

However, headquarters officials we interviewed at CEOS, ICE, and USSS disagreed on the need for such additional steps because they believe the additional steps are not needed to support a successful prosecution and the steps increase the costs and time needed for analysis to take place, thereby further increasing backlogs. All of these officials stated that they do not routinely incorporate all of these additional steps because they do not believe that the addition of these extra steps would discernibly impact the overall integrity of the forensic analysis.⁷⁴ For example, these officials stated that it is not necessary to separate examiners who extract digital evidence from hard drives from law enforcement agents who review the extracted information; evidence of a suspect's guilt on his or her hard drive is either present or not. These officials noted that unlike other areas of forensic analysis, such as footprint or hair analysis where there is a concern that bias may impact interpretations of results, there is little opportunity for bias on the part of the forensic examiner to affect the results of an investigation. They all added that the steps already in place, specifically copying and taking hash values of original evidence, ensure that any effort to alter the material on a suspect's hard drive would be detected.

Six of the seven prosecutors we spoke with stated that they were generally indifferent as to which federal law enforcement agency conducted forensic examinations, and there was no discernable difference in the quality or usefulness of forensic analysis conducted by the different agencies. However, headquarters prosecutors we interviewed stated that the time it takes to receive reports from different agencies varies by district nationwide. In addition, these officials noted that there were differences in the content and subjectivity of the forensic reports that

⁷⁴CEOS officials stated that they do not require forensic analysts to record search activities; however, they may do so at their own discretion. Additionally, USSS labs conduct peer reviews of forensic reports before they are released.

agencies prepared to present examination results. For example, they opined that reports that included detailed information about how the forensic examination was conducted, what was found, and what it means provide prosecutors with more useful data, and one prosecutor indicated that he preferred the format of forensic reports used by some law enforcement agencies over others.

While these variations exist, senior DOJ officials noted that the government's analysis of digital evidence is repeatedly subjected to challenges in court when the government puts on its case, and must be determined by a judge to meet standards for admissibility. These officials noted that CEOS computer forensic specialists conduct forensic analysis of digital evidence in cases prosecuted across the country and have presented the results in court frequently over the last several years in numerous cases; however, DOJ is unaware of such evidence being suppressed or ruled inadmissible by any court in any case due to a lack of integrity in the forensic analysis process. According to DOJ headquarters prosecutors, this indicates that the forensic analysis provided by all federal law enforcement agencies to support prosecutions of offenders has incorporated a sufficient amount of integrity into the process.

DOJ Working Group Could Assess the Costs and Benefits of Forensic Analysis Steps to Identify Efficiencies

DOJ convened a working group in August 2010, coinciding with the publication of the National Strategy, to carry out elements of the strategy, and this working group established a Technical Assistance Subcommittee, which is responsible for examining technological issues related to combating child exploitation, including forensic analysis of digital evidence. The Act requires DOJ to include in its National Strategy a review of the backlog of forensic analysis for child exploitation cases and plans for reducing the forensic backlogs.⁷⁵ In response to this requirement, the subcommittee is examining forensic analysis of digital evidence, including efforts to reduce backlogs.⁷⁶ Specifically, according to the National Coordinator, the working group is reviewing different methods used among the federal agencies to identify practices that may reduce backlogs, such as increased review of computers within a suspect's residence before

⁷⁵Pub. L. No. 110-401, § 101(c)(10)–(11).

⁷⁶In addition to the subcommittee's efforts, federal law enforcement agencies have reported taking steps to address backlogs. For example, USSS officials stated that the agency has sent teams of examiners to field locations to address backlogs in specific offices. The FBI has developed kiosks that allow agents to review evidence in a forensically sound manner without sending evidence to a forensics lab for analysis.

taking them to a laboratory for forensic examination. However, the National Coordinator said that such a review will not explicitly assess the costs and benefits of steps taken by federal agencies to ensure the integrity of the forensic examination process or the separation of the examination and investigative functions in forensic analysis. Specifically, the working group does not currently plan on assessing whether any enhancement of the credibility of digital evidence resulting from steps taken by federal law enforcement agencies to ensure the integrity of the forensic examination process will outweigh the costs associated with performing these additional steps, such as whether backlogs that may result from implementing these steps will allow offenders to remain on the street for a longer amount of time while evidence is being forensically examined.

Differences in steps for conducting forensic analysis of digital evidence exist; however, no federal agency or working group we spoke to has assessed the costs and benefits of steps taken to ensure the integrity of forensic analysis used by federal law enforcement agencies that investigate and prosecute online child pornography crime due to an overall satisfaction with their own individual digital forensic examination processes to date. OMB cites assessments of costs and benefits as key in the consideration of alternative means of achieving program objectives by examining different program methods. OMB also states that these assessments that serve as a basis for evaluating government programs or policies should identify societal costs and benefits, as well as discuss any trade-offs that may not be quantifiable.⁷⁷ For example, this could include examining qualitative factors—such as delays in arrest and prosecution, which may expose the public to offenders and concerns regarding the integrity of forensic analysis conducted by the government, which could impact the credibility of evidence presented in federal prosecutions—as well as quantitative factors such as financial costs of conducting forensic analysis of digital evidence.

According to the DOJ's National Coordinator, the Working Group and its Technical Assistance Subcommittee are in a good position to address backlog issues due to its multiagency membership.⁷⁸ As the Working

⁷⁷See Circular No. A-94 *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs* (October 1992).

⁷⁸The Working Group includes members from FBI, CEOS, ICE, USISP, five ICAC task forces, the Executive Office for United States Attorneys, Department of Defense, and USSS.

Group and its Technical Assistance Subcommittee review different methods of reducing backlogs, assessing the costs and benefits of steps taken to ensure the integrity of forensic analysis, including impacts on timeliness of analysis, could help it to determine potential efficiencies while providing a level of assurance that evidence is presented consistently and is of high quality. This assessment could involve reviewing steps, such as creating copies of digital evidence and separating examination and investigation functions, and determining whether, and to what extent, these steps enhance the credibility of forensic review and do not create undue backlogs. Such an assessment could further provide assurance to law enforcement agencies that conduct forensic analysis of digital evidence that scarce forensic resources are being allocated in a way that maximizes their efficiency and effectiveness.

ESP Data Retention Is a Concern, but Officials We Interviewed Were Generally Able to Obtain Data from ESPs or through Other Means

According to CEOS, FBI, ICE, and USSS headquarters officials, data from ESPs, such as IP addresses, can be traced back to offenders, and this information is often key to investigations of online child pornography crime. In June 2010, the Online Safety and Technology Working Group (OSTWG) reported that data retention—the period of time ESPs retain data entered or transmitted by users to their networks—is a very contentious issue with competing needs and concerns from law enforcement, the Internet industry, and consumer privacy advocates.⁷⁹ Currently, unlike data included in reports to NCMEC, ESPs are generally not required to retain user data not reported to NCMEC that could provide investigators evidence for any specified amount of time.⁸⁰ According to OSTWG’s report, the perspective of law enforcement is that mandatory data retention sufficient to facilitate investigations of online crimes would allow law enforcement to solve more crimes involving the sexual exploitation of children because more information from ESPs would be available to support investigations. Similarly, in January 2011, a Deputy Assistant Attorney General within DOJ testified that data retention is fundamental to the department’s work in investigating and prosecuting

⁷⁹OSTWG was established by the Protecting Children in the 21st Century Act to evaluate the data retention practices of ESPs, among other things. Pub. L. No. 110-385 § 214, 122 Stat. 4096, 4103-04 (2008).

⁸⁰As noted earlier in the report, an exception to this general rule is that ESPs are automatically required to preserve the contents of any report to NCMEC’s CyberTipline, as well as any commingled images or data, for 90 days. 18 U.S.C. § 2258A(h). In addition, law enforcement may direct an ESP to preserve existing records or other evidence for a renewable period of 90 days. 18 U.S.C. § 2703(f).

almost every type of crime. He stated, for example, that in one case, investigators sent legal process—such as a subpoena, court order, or search warrant—to ESPs seeking to identify distributors of child pornography based on IP addresses that were 6 months old or less. Of the 172 requests, they received 33 responses (about 19 percent) noting that the requested information was no longer retained by the company because it was out of their data retention period.⁸¹

Alternatively, the OSTWG report stated that the industry perspective is that, while the cost of data storage has fallen over the years, the true cost of data retention comes from having to protect increasing amounts of users' private data from online criminals who may try to access this information to commit crimes, such as identity theft. Similarly, Internet and consumer privacy advocates testified about concerns with mandatory data retention. For example, in January 2011, the executive director of the U.S. Internet Service Provider Association testified before Congress that a data retention mandate would bring with it a complex regulatory framework that would impose new and unforeseen costs, legal risks, and burdens to the Internet industry.⁸² Also in January 2011, an official from the Center for Democracy and Technology testified that mandatory data retention requirements would aggravate the problem of identity theft and damage competition and innovation in the Internet industry.⁸³

However, headquarters law enforcement officials we spoke with from FBI, CEOS, and ICE, as well as officials from eight of the ICAC task forces, all stated that current ESP data retention periods may be insufficient to facilitate investigations and prosecutions of online child pornography

⁸¹Statement of Jason Weinstein, Deputy Assistant Attorney General, Criminal Division. Hearing on "Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes," before the U.S. House of Representatives, Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security, January 25, 2011.

⁸²Statement of Kate Dean, United States Internet Service Provider Association. Hearing on "Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes," before the U.S. House of Representatives, Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security, January 25, 2011.

⁸³Statement of John B. Morris, Jr., Center for Democracy and Technology. Hearing on "Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes," before the House Committee on the Judiciary, Subcommittee on Crime, Terrorism and Homeland Security, January 25, 2011. The Center for Democracy and Technology is a nonprofit public interest organization dedicated to keeping the Internet open, innovative, and free.

crime.⁸⁴ Specifically, all of these officials stated that data—such as IP addresses and any corresponding user information which an address may help identify (i.e., name, credit card, and bank account number)—allow law enforcement to identify who possessed, distributed, and manufactured images of child pornography. For example, according to ICE Cyber Crimes Center officials we spoke with, if an offender subscribes to a Web site that sells child pornography, the IP address of the computer associated with that suspect and transaction can be traced back to an individual offender. According to these officials, a law enforcement agency can subpoena an ESP for identifying information, such as name and address, for the individual who had that IP address at the time that the transaction took place.⁸⁵ However, in some instances, there is a gap in the amount of time between when a child pornography offense occurs and when it is detected by law enforcement. If the ESP does not maintain information on which of its users was associated with a particular IP address, law enforcement will likely not be able to obtain this information, in which case an investigation may not be able to proceed.

Officials from 17 of the 19 ESPs we spoke with stated that in general their data retention policies were based on business considerations, such as the types of services provided.⁸⁶ For example, officials from 4 ESPs that offered paid services, such as Internet connectivity, stated that they keep billing information, such as address or payment history, indefinitely, while officials from 3 ESPs that operate social networking sites stated that they keep user data until the user cancels his or her account. We discussed the extent to which they were able to obtain information from ESPs they contacted with officials from the eight ICAC task forces we selected. Officials from six of the eight said they were able to obtain information from ESPs that enabled them to further their investigations about 80

⁸⁴DOJ's National Coordinator stated that DOJ has not taken a position regarding the need for data retention requirements. The International Association of Chiefs of Police passed a resolution in 2006 calling for the development of appropriate but uniform data retention requirements for ESPs to require, among other things, the retention of customer subscriber information for a minimum specified period of time so that it will be available to the law enforcement community.

⁸⁵See 18 U.S.C. § 2703(c)(2). Law enforcement can also request that the ESP preserve stored records and communications for a period of 90 days, which is renewable upon request. 18 U.S.C. § 2703(f).

⁸⁶Two ESPs opted to not provide information on their data retention policies.

percent of the time or more.⁸⁷ In addition, officials from these six task forces stated that when they were not able to obtain information from an ESP, they were generally able to obtain relevant information—such as IP addresses or image data—through other means, such as by interviewing suspects at their residences or reviewing information on their computers.

According to the OSTWG report, there is not a consensus on whether any data retention mandates should be imposed on ESPs. Such mandates would require legislative action. The report concluded that data retention is about striking a balance among (1) law enforcement’s legitimate need to investigate and prosecute crimes against children carried out or facilitated by the Internet; (2) end users’ legitimate privacy expectations; and (3) ESPs’ cost of data retention, costs which ultimately get passed onto consumers.

Conclusions

With dramatic increases in the numbers of online child pornography offenders and new technologies and tools that these offenders can use to produce and distribute child pornography, Congress passed the PROTECT Our Children Act of 2008 and DOJ and NCMEC are responding to the provisions of the Act. However, DOJ has not implemented three provisions—that address studying the potential danger posed by child pornography offenders, designating foreign law enforcement agencies that can receive reports from NCMEC’s CyberTipline, and developing a report on DOJ’s information-sharing structure—and has not yet established specific plans or time frames for doing so. Developing steps and time frames for fulfilling these three provisions, as required, may also help better ensure that law enforcement resources are more optimally focused on dangerous offenders as well as help ensure that investigative information is disseminated on a timelier basis. Also since passage of the Act, NCMEC has developed guidance for ESPs to help them in reporting tips and has played a key role in coordinating law enforcement efforts through the operation of its CyberTipline. However NCMEC could take steps to enhance the feedback it receives from law enforcement on the usefulness of CyberTipline reports. Doing so could help NCMEC ensure that these reports consistently contain as much information as possible to help law enforcement take actions, such as advancing investigations, which is critical given the increase in the number of CyberTipline reports.

⁸⁷Officials from two ICACs did not provide information about how often they were able to obtain information from ESPs.

Finally, key to every investigation and prosecution of online child pornography crime is forensic analysis of digital evidence. Among the factors that federal law enforcement officials cited as limiting investigations and prosecutions were variations in the steps that agencies believe enhance integrity of forensic analysis of digital evidence. In some cases, these steps may increase the time it takes to analyze evidence and add to backlogs and delays. DOJ's working group examining forensic issues, due to its multiagency composition, is in a position to assess the costs and benefits of steps taken by different agencies to ensure the integrity of forensic processes. Such an assessment could help identify possible efficiencies in these steps and provide assurance to law enforcement agencies that conduct forensic analysis of digital evidence that scarce forensic resources are being allocated in a way that maximizes their efficiency and effectiveness.

Recommendations

To help ensure that DOJ fulfills its obligations as outlined in the PROTECT Our Children Act of 2008 as well as enhance its ability to address online crimes against children, we recommend that the Attorney General define the steps it plans to take and time frames for completing the three provisions of the Act that it has not yet implemented.

To help ensure that NCMEC maximizes the feedback it receives from law enforcement agencies about the usefulness of CyberTipline reports in initiating and advancing investigations, we recommend that NCMEC's Chief Executive Officer work with its law enforcement customers to enhance its processes to collect feedback from law enforcement about the usefulness and quality of individual CyberTipline reports and use this information to make any necessary improvements it identifies.

To help address backlogs in forensic analysis of digital evidence conducted in support of investigations and prosecutions of online child pornography crime, we recommend that the Attorney General direct the National Strategy Working Group and its Technical Assistance Subcommittee to assess the costs and benefits of the various steps federal law enforcement agencies believe enhance the integrity of forensic analysis of digital evidence in investigating online child pornography crimes, which may be quantitative or qualitative, to identify any efficiencies in the processes agencies use to help them to make more informed decisions on the efficient allocation of limited forensic resources.

Agency Comments, Third Party Views, and Our Evaluation

We provided a draft of this report to DOJ, NCMEC, DHS, and USPIS for review and comment. DOJ and NCMEC provided written comments, which are reprinted in appendix IV and V and evaluated below. In commenting on our draft report, DOJ stated that it generally concurred with our recommendations and discussed actions it had taken or plans to take, which address in part, our recommendations.

DOJ concurred with our first recommendation to define the steps it plans to take and time frames for completing three provisions of the Act and outlined efforts to address the provisions. For example, in terms of the requirement for NIJ to prepare a report to identify the factors indicating whether the subject of an online investigation poses a high-risk of harm to children, DOJ noted that the grantee selected to develop NIDS would, as part of this effort, provide a paper addressing the dangers posed by child pornography offenders and recommending further research paths. Documentation provided by DOJ indicated that the grantee, as part of the development of the NIDS system would, among other things, conduct a literature review about the links between child pornography and hands-on molestation and develop a research design to address gaps in assessing dangers from child pornography offenders. While these activities are important steps to providing law enforcement with additional information on potential dangers posed by offenders, it will be important for DOJ to ensure that the grantee's efforts or follow-on research comply with statutory requirements—that DOJ identify factors that indicate whether the subject of an online investigation poses a high-risk of harm to children as well as to coordinate with federal law enforcement agencies, NCMEC, and other stakeholders, as required by the Act. Similarly, to address the provision of the Act requiring a report to congressional committees related to information sharing structures, DOJ noted that it has secured a grantee to provide a design for an information sharing system, and when the system is closer to fruition, DOJ plans to report to Congress on its progress. While these are important steps, we maintain that it will also be important for DOJ to commit to plans and timeframes to hold itself accountable for fulfilling these provisions of the Act.

DOJ concurred with our recommendation to assess the costs and benefits of steps taken by federal law enforcement agencies that they believe enhance the integrity of the forensic analysis of digital evidence, with one modification. In discussions with DOJ's National Coordinator as well as senior FBI officials responsible for overseeing forensic analysis of digital evidence on this recommendation, officials indicated that they had concerns regarding the proposed recommendation to assess costs and benefits of the processes various federal law enforcement agencies

undertake that are believed to enhance the integrity of the forensic analysis of digital evidence. For example, these officials noted that certain costs associated with potential backlogs in forensic analysis, such as the public's increased exposure to offenders, would be very difficult to quantify. We explained that we did not intend for DOJ to conduct this level of cost-benefit analysis and develop such quantifiable dollar estimates, but rather intended for DOJ to qualitatively assess, for example, whether the costs, such as increasing backlogs in forensic analysis, are outweighed by the perceived benefits of the extra steps agencies take to enhance the integrity of the forensic analysis process for this particular crime. Thus, we modified our recommendation to clarify this point.

Related to this recommendation, in its comments, DOJ described two working groups currently addressing forensic issues—the Technical Assistance Subcommittee, which has been studying the timeliness and usefulness of forensic examinations and has recommendations under agency review, and the Office of the Deputy Attorney General's Computer Forensics Working Group, which is also examining current digital forensic processes. DOJ noted that these groups plan to take into account the resources associated with various steps DOJ law enforcement takes in conducting digital forensic analysis as part of their examinations. DOJ also noted that it hopes to be able to provide an update to Congress on its progress on digital forensic analysis by about September 2011. We maintain that these groups and their efforts could be the appropriate vehicle to use to conduct the assessment of costs and benefits called for in our recommendation. Doing so could help identify possible efficiencies in agencies' digital forensic analysis processes, ensure scarce forensic resources are allocated to maximize their efficiency and effectiveness, and ultimately, help better address online child sexual exploitation.

NCMEC, in its comments, also concurred with our recommendation to enhance its processes to collect feedback from law enforcement agencies about the usefulness of CyberTipline reports. NCMEC stated that it would further its efforts to solicit better feedback from law enforcement on the usefulness of these reports. In addition, NCMEC agreed that better understanding how information ESPs provide may determine whether a law enforcement agency can begin an investigation would be helpful. DOJ also noted in its comments that efforts to improve the CyberTipline process are underway, and the department plans to work with NCMEC to report to Congress on these improvements by about September 2011.

Finally, DOJ also provided us with technical comments, which we incorporated into the report, as appropriate. DHS did not provide

comments on our report. In an email dated March 16, 2011, the USPIS Acting Assistant Inspector in Charge for child exploitation investigations concurred with the information in the report and provided technical comments, which we incorporated into the report, as appropriate.

We are sending copies of this report to the Secretary of Homeland Security, the Attorney General, the Executive Director of NCMEC, and other interested congressional committees and subcommittees. In addition, this report will be available at no charge on GAO's Web site at <http://www.gao.gov>. If you or your staff have any questions concerning this report or wish to discuss the matter further, please contact me at (202) 512-8777, or larencee@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix VI.



Eileen Regen Larence
Director, Homeland Security
and Justice Issues

Appendix I: Key Federal Agencies Involved in Combating Online Child Pornography

Appendix I provides information about the mission, role, level of resources, and trends in investigations or cases initiated for key federal agencies involved in combating online child pornography.

Department of Justice

Federal Bureau of Investigation

The Federal Bureau of Investigation (FBI) investigates various crimes against children, including online child pornography. For example, FBI investigates violations of federal statutes generally relating to:

- producing child pornography;
- permitting a minor within one’s custody or control to be used in child pornography;
- selling or buying children for use in child pornography; and
- transporting, shipping, receiving, or distributing child pornography by any means, including by computer.

As shown in tables 3 and 4, the amount of personnel and fiscal resources the FBI has allocated to combating child exploitation crime, including child pornography, increased from fiscal year 2006 through fiscal year 2010.¹

Table 3: FBI Personnel Dedicated to Combating Child Exploitation

Number of personnel				
FY 2006	FY 2007	FY 2008	FY 2009	FY 2010
267	283	315	318	313

Source: FBI.

Note: Represents agents from FBI’s Crimes against Children and Innocent Images National Initiative units.

¹Pursuant to the Providing Resources, Officers, and Technology To Eradicate Cyber Threats to Our Children Act of 2008 (PROTECT our Children Act of 2008), “child exploitation” generally consists of conduct involving a minor that violates specific criminal provisions of the U.S. Code, or any sexual activity involving a minor for which a person can be charged with a criminal offense. Pub. L. No. 110-401, § 2, 122 Stat. 4229, 4230. Some of these criminal provisions include, for example, causing a minor to engage in a sex act by force; transporting an individual for purposes of prostitution or other criminal sexual activity; or mailing, receiving, and distributing child pornography. Child pornography has a more specific definition under 18 U.S.C. § 2256, and generally consists of any visual depiction, the production of which involves the use of a minor engaging in sexually explicit conduct or that involves a minor engaging in sexually explicit conduct.

Table 4: FBI Resources Obligated for Combating Child Exploitation

Dollars in millions				
FY 2006	FY 2007	FY 2008	FY 2009	FY 2010
45.5	47.4	54.4	62.7	62.9

Source: FBI.

Note: Represents funds obligated by FBI's Innocent Images National Initiative unit.

Innocent Images National Initiative

The FBI established a nationwide initiative to combat the proliferation of online child sexual exploitation. The Innocent Images National Initiative (Innocent Images), a component of the FBI's Cyber Division, is a proactive, investigative initiative whose mission is to combat the proliferation of child pornography facilitated by computer. This initiative is composed of agents working at regional offices nationwide and may involve agents from any of the FBI's 56 field offices. Innocent Images provides centralized coordination and analysis of case information that is national and international in scope and requires coordination with state, local, and international governments as well as among FBI field offices and legal attaches. Its mission is to:

- identify, investigate, and prosecute sexual predators who use the Internet and online services to sexually exploit children;
- establish a law enforcement presence on the Internet as a deterrent to subjects that use the Internet to exploit children; and
- identify and rescue witting and unwitting child victims.

As shown in table 5, FBI child pornography investigations and arrests have increased from fiscal years 2006 through 2010.

Table 5: Number of FBI Child Pornography Investigations and Arrests

Number	Fiscal year				
	2006	2007	2008	2009	2010
Investigations	4,467	4,952	5,667	6,062	6,070
Arrests	936	1,115	1,144	1,077	1,094

Source: FBI.

Child Exploitation and Obscenity Section

The Child Exploitation and Obscenity Section (CEOS) is a unit within the Department of Justice's (DOJ) Criminal Division that specializes in the prosecution of federal child sexual exploitation offenses. Among other things, CEOS is primarily responsible for the development of prosecution, policy, and legislative initiatives in those areas. CEOS's professional staff

consists of attorneys and computer forensics specialists in CEOS's High Technology Investigative Unit dedicated to combating the sexual exploitation of children and obscenity. Established in 1987, CEOS focuses on individuals who, in the context of child exploitation:

- possess, manufacture, produce, or traffic in child pornography;
- travel interstate or internationally to sexually abuse children, or cause children to travel interstate or internationally for that same purpose;
- use the Internet to lure children to engage in prohibited sexual conduct;
- abuse children on federal and Indian lands; or
- engage in domestic child sex trafficking.

CEOS attorneys work closely with federal law enforcement agencies and prosecutors on investigations, trials, and appeals. As shown in tables 6 and 7, the amount of fiscal resources at CEOS dedicated to combating child exploitation, including resources available to assist with and prosecute child pornography and obscenity related cases, grew from fiscal year 2006 through fiscal year 2010, while CEOS's personnel resources fell over that same period.

Table 6: CEOS Personnel Dedicated for Combating Child Exploitation and Obscenity Offenses

Number of personnel				
FY 2006	FY 2007	FY 2008	FY 2009	FY 2010
36	32	32	32	32

Source: DOJ's Criminal Division.

Table 7: CEOS Funds Obligated for Combating Federal Child Exploitation and Obscenity Offenses

Dollars in millions				
FY 2006	FY 2007	FY 2008	FY 2009	FY 2010
4.4	4.8	5.3	5.9	5.9

Source: DOJ's Criminal Division.

Office of Juvenile Justice and Delinquency Prevention: Internet Crimes Against Children Program

Created by DOJ in 1998, the Internet Crimes Against Children (ICAC) program, administered and funded through the Office of Juvenile Justice and Delinquency Prevention (OJJDP), encourages communities nationwide to develop regional, multijurisdictional, and multiagency responses to Internet crimes against children. The program provides grants to state and local law enforcement agencies to build regional task forces that address and combat Internet-related crimes against children.

ICAC program grants can be used to ensure that investigators receive specialized training and technological resources to combat Internet-related crimes. Additionally, ICAC task forces have been established to serve as sources of prevention, education, and forensic investigative assistance to those who work to address Internet crimes against children. ICAC's objectives include:

- developing or expanding multiagency, multijurisdictional task forces that include representatives from law enforcement, prosecution, victim services, and child protective services, among others;
- ensuring investigative capacity by properly equipping and training ICAC task force investigators;
- developing and maintaining case management systems to document reported offenses and investigative results; and
- developing response protocols or memorandums of understanding to foster collaboration, information sharing, and service integration among public and private organizations to protect children from being sexually exploited.

A number of federal agencies are also involved in the ICAC Task Force Program through membership on various task force units and through participation on the ICAC Task Force Board. These partners include DOJ's CEOS, FBI, the Executive Office for United States Attorneys, Immigration and Customs Enforcement (ICE), and the United States Postal Inspection Service (USPIS).

As shown in table 8, the number of ICAC task force child exploitation investigations and arrests increased from fiscal year 2006 through 2010.

Table 8: Number of ICAC Task Force Child Exploitation Cases Investigated and Arrests

Number	Fiscal year				
	2006	2007	2008	2009	2010
Cases investigated	10,800	14,700	21,700	22,700	32,300
Arrests	2,100	2,500	3,100	4,500	5,300

Source: OJJDP.

Note: Prior to the enactment of the PROTECT Our Children Act of 2008, OJJDP did not require ICAC task forces to track investigations data. The agency provided estimates for investigations totals for fiscal years 2006 through 2008, based on multiple variables including arrests and closed investigations among other factors.

Department of Homeland Security

U.S. Immigration and Customs Enforcement

U.S. Immigration and Customs Enforcement (ICE) was one of the first federal law enforcement agencies to combat the sexual exploitation of children. Beginning in the 1970s, ICE, under the legacy U.S. Customs Service, used its unique customs and border authority to investigate individuals and groups that were introducing child pornography into the United States. Since 2003, ICE has continued this effort through enforcement of trans-border violations of federal child exploitation statutes, including those related to child pornography. The agency becomes involved in cases with foreign links, primarily focusing on child pornography that enters the United States from abroad. In addition, ICE investigates, interdicts, and prosecutes those individuals involved in, among other things:

- possession, receipt, distribution, advertisement, transportation, and production of child pornography;
- trafficking of children for sexual purposes; and
- traveling in foreign commerce to engage in sexually explicit conduct with minors (also known as sex tourism).

ICE's Office of Investigations established the Cyber Crimes Center to more effectively focus ICE resources on Internet crimes. The center brings together all ICE resources dedicated to the investigation of international criminal activity conducted on or facilitated by the Internet, including the sharing and distribution of child pornography. The center also trains personnel and upgrades their techniques to combat the diverse ways in which offenders download, possess, and distribute child pornography. The center acts as a clearinghouse and directs investigations to applicable areas within the United States and foreign countries. Through the Cyber Crimes Center, ICE addresses smuggling over "traditional" borders as well as smuggling associated with the Internet.

As shown in tables 9 and 10, the amount of personnel and fiscal resources the ICE has allocated to combating child exploitation crime, including child pornography, increased from fiscal year 2006 through fiscal year 2010.

Table 9: ICE Personnel Dedicated for Combating Child Exploitation

Number of personnel				
FY 2006	FY 2007	FY 2008	FY 2009	FY 2010
208.7	211.8	228.3	227	239.3

Source: ICE.

Note: Represents agent data manually derived from ICE field offices through September 30, 2010.

Table 10: ICE Resources Obligated for Combating Child Exploitation

Dollars in millions				
FY 2006	FY 2007	FY 2008	FY 2009	FY 2010
0.531	1.32	0.916	0.724	0.951

Source: ICE.

Note: Represents manually derived estimates of funds obligated by ICE field offices through September 30, 2010.

As shown in table 11, the number of ICE child pornography cases initiated has decreased, while arrests have increased from fiscal years 2006 through 2010.

Table 11: Number of Child Pornography Cases Initiated and Arrests by ICE Agents

Number	Fiscal year				
	2006	2007	2008	2009	2010
Cases initiated	3,291	3,191	2,898	2,894	2,622
Arrests	681	948	863	957	931

Source: ICE.

United States Secret Service

The United States Secret Service (USSS) provides forensic and technical assistance in matters involving missing and sexually exploited children through its Office of Investigations. The USSS' Forensic Investigative Response and Support Team consists of a group of technical and forensic experts, including agents from the Electronic Crimes Special Agent Program, who are available to respond to requests from any law enforcement agency within the United States to perform forensic and technical examinations. Section 105 of the USA Patriot Act requires USSS to develop a national network of electronic crime task forces to combat

various forms of electronic crimes.² In response to this requirement, USSS has established 31 regional Electronic Crimes Task Forces worldwide. The regional task forces work directly with other federal, state, and local law enforcement agencies in the area of child pornography as well as other electronic crimes.

According to USSS headquarters officials, online child pornography crime is not a core violation for the agency. Therefore, it has pursued fewer investigations involving this crime than other crimes, such as counterfeiting, and does not track funding or personnel dedicated to this crime. These officials added, however, that some USSS field offices with a background in these areas as well as digital forensic capabilities investigate these crimes. As shown in table 12, while the number of investigations has varied over time, the number of arrests related to child pornography has increased.

Table 12: Number of USSS Investigations and Arrests Related to Child Pornography

Number	Fiscal year				
	2006	2007	2008	2009	2010
Investigations	302	487	138	98	188
Arrests	88	94	80	88	149

Source: USSS.

United States Postal Service

United States Postal Inspection Service

The United States Postal Inspection Service (USPIS) is the federal law enforcement arm of the United States Postal Service that is responsible for investigating crimes involving the U.S. mail, including child pornography and child sexual exploitation offenses. Postal Inspectors, specially trained to conduct child exploitation investigations, are assigned to each of its 18 field divisions nationwide. The use of mail to traffic in child pornography, or to sexually exploit children, continues to be a significant societal problem, according to Postal officials. They added that the exchange of child pornography by mail is now often preceded by use of the Internet to

²Pub. L. No. 107-56, 115 Stat. 272, 277 (2001).

communicate with like-minded individuals or to locate sources of child pornography.

The objective of the child exploitation program is to reduce and deter the use of the postal system for the procurement or delivery of materials that promote the sexual exploitation of children and to uphold customer confidence. In carrying out its mission, USPIS works with DOJ, FBI, ICE, and other national and international law enforcement agencies.

As shown in table 13, the number of full-time Postal Inspectors dedicated to combating child exploitation has decreased overall; however, the number of inspectors addressing these crimes on a part-time basis has increased.

Table 13: Full Time and Part Time Postal Inspectors Assigned to Child Exploitation Investigations

Number of postal inspectors					
	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010
Full time	37	37	38	36	26
Part time	0	0	10	14	19

Source: USPIS.

According to USPIS, as a result of its transformation and reorganization during the past 2 years, it assigned fewer full-time Postal Inspectors to investigate child exploitation in a proactive manner, yet increased the assignment of part-time Postal Inspectors to ensure any lead referred to the division is addressed. As shown in table 14, the number of investigations related to child exploitation and child pornography has decreased. According to USPIS, Postal Inspectors are now focused on high-quality U.S. mail-related investigations involving the sexual exploitation of children, and investigations not involving the U.S. mail (e.g., those that are Internet-related) are now being worked at a significant rate by partners, such as the ICAC task forces.

Table 14: Postal Inspection Service Investigations and Arrests Related to Child Exploitation and Child Pornography

Number	Fiscal year				
	2006	2007	2008	2009	2010
Investigations	267	264	310	233	141
Arrests	252	155	165	186	115

Source: USPIS.

Appendix II: Status of Efforts of DOJ and NCMEC's CyberTipline to Implement Provisions of the PROTECT Our Children Act of 2008

Table 15 presents information on the actions taken by DOJ and NCMEC to implement their responsibilities under the Providing Resources, Officers, and Technology To Eradicate Cyber Threats to Our Children Act of 2008 (PROTECT Our Children Act of 2008, or the Act).¹

Table 15: Status of Efforts of the Attorney General and NCMEC's CyberTipline to Implement Their Responsibilities under the PROTECT Our Children Act of 2008

Responsible entity or official	Provision	Responsibility	Status of effort
Attorney General	§ 101(a) – (c); 42 U.S.C. § 17611(a) – (c).	National Strategy for Child Exploitation Prevention and Interdiction: Due 1 year after the date of enactment, and every second year thereafter. The statute requires that the Strategy contain 19 elements, including goals and measurable objectives, a review of DOJ's work, plans for interagency coordination—with ICE and the Departments of State, Commerce and Education, among others—a review of the ICAC Task Force Program, a review of and plans for reducing forensic backlogs, and a review of all available statistical data on child pornography trafficking, among other elements.	In August 2010, DOJ released its National Strategy for Child Exploitation Prevention and Interdiction (National Strategy). This document contained elements specified for inclusion by the PROTECT Our Children Act of 2008, including a review of DOJ work related to the prevention and investigation of child exploitation crime, a review of the ICAC Task Force program, a review of the backlog of forensic analysis for child exploitation cases, and plans for reducing the forensic backlog. In terms of plans for updating the National Strategy, DOJ officials stated that they are currently working on implementation of the National Strategy, which was submitted in August. As they move forward with implementation, they said that they plan to decide whether the goals and priorities need to be updated. In addition, they are updating the National Strategy with information from each agency and component. The officials stated that DOJ plans to submit the National Strategy to Congress by April 1, 2011.
Attorney General	§ 101(d); 42 U.S.C. § 17611(d).	Designation of Senior Official: The Attorney General must designate a DOJ senior official to be responsible for the strategy, who must act as a liaison with other federal entities, ensure proper coordination, be knowledgeable about relevant DOJ budget priorities and efforts, and be available to Congress.	DOJ designated a Senior Official responsible for development of the National Strategy on January 13, 2010. To facilitate the role as a liaison with other federal entities, the National Coordinator has called together a multiagency National Strategy Working Group to work on implementing the National Strategy. This working group includes participants from DHS, the Department of State, the Department of Defense, USPIS, the Department of Commerce, the Department of Education, Commanders from four ICAC Task Forces, as well as various components of DOJ, including FBI, CEOS, the OJJDP, and U.S. Attorneys' Offices. There are six subcommittees under the Working Group that are responsible for implementing various components of the National Strategy. They are subcommittees on Technical Assistance, Global Outreach, Community

¹Pub. L. No. 110-401, 122 Stat. 4229.

**Appendix II: Status of Efforts of DOJ and
NCMEC's CyberTipline to Implement
Provisions of the PROTECT Our Children Act
of 2008**

Responsible entity or official	Provision	Responsibility	Status of effort
Attorney General	§§ 102-04; 42 U.S.C. §§ 17612-14.	<p>ICAC Task Force Program: Establishes in law the ICAC Task Force Program, under the authority of the Attorney General, which is a national program of state and local law enforcement task forces dedicated to developing responses to online enticement of children by sexual predators, child exploitation, and child obscenity and pornography cases. The statute requires that there be at least one task force per state and that the Attorney General consult with and consider the 59 task forces in existence at time of enactment in establishing the program. Requires the Attorney General to conduct periodic review of the effectiveness of each task force and authorizes the Attorney General to establish new task forces, subject to certain conditions. Grants authority to the Attorney General to conduct training; requires periodic review of the effectiveness of training; limits training awards to any one entity to \$2 million annually. Includes 9 specified purposes of the task forces and 11 required functions and duties, 1 of which includes working toward achieving the purposes.</p>	<p>Outreach, Research and Grant Planning, Training, and Law Enforcement Collaboration.</p> <p>There is currently at least one ICAC per state. Since the passage of the PROTECT Our Children Act of 2008, 2 new ICAC task forces have been formed, 1 in Houston and 1 in New York City—for a total of 61 ICAC task forces. According to DOJ officials, in general, solicitations for grants for new ICAC task forces were announced approximately 6 months before grant recipients were selected. Approximately 10 days before local entities in the Houston and New York areas were notified that their grant proposals were accepted, Congress was notified of the grant selections.</p> <p>According to DOJ officials, assessments of ICAC performance are done on a monthly and quarterly basis. The information collected includes data on number of arrests and investigations, community education programs, and other factors.</p> <p>According to DOJ officials, DOJ was already collecting from the ICAC task forces and reviewing many data points required by the PROTECT Our Children Act of 2008. A DOJ official stated that the Act included a new requirement that DOJ collect information on the number of investigations conducted. This new data point was incorporated into ICAC program management in 2009-2010. DOJ noted that the ICAC task forces are now required to submit data on these new data points, and program managers review the data submitted. DOJ provides spreadsheets to ICAC task forces listing these and other required data points that are then submitted to OJJDP.</p> <p>In March 2010, DOJ's Office of Audit, Assessment, and Management reviewed the ICAC Technical and Training Assistance program and found that, based on student evaluations and observations, the overall quality of training provided was of high quality and well-received. However, the IG noted concerns with the management of OJJDP's training program. Specifically, the IG reported that OJJDP performance measures for the effectiveness of the training program were output based and did not measure the long-term effectiveness of the training program.</p> <p>To conduct periodic assessments, according to DOJ officials, OJJDP collects posttraining reviews on training programs conducted under the ICAC training program. Officials said that OJJDP conveyed the requirement to training grant recipients in 2009 and 2010 that they must provide immediate and long-</p>

**Appendix II: Status of Efforts of DOJ and
NCMEC's CyberTipline to Implement
Provisions of the PROTECT Our Children Act
of 2008**

Responsible entity or official	Provision	Responsibility	Status of effort
Attorney General	§ 106(a) – (c); 42 U.S.C. § 17616(a) – (c).	ICAC Grant Program: Authorizes the Attorney General to award grants to ICAC task forces, pursuant to statutory factors and criteria. In order to receive funds, task forces must submit applications, describing uses of funds; funds may only be used for specified allowable uses.	<p>term reviews of training efficacy. These assessment efforts are paid for with existing DOJ funding. OJJDP also reviews semiannual progress reports and deliverables produced under every ICAC training program grant.</p> <p>DOJ officials stated that even though the Act authorized up to \$60 million per year to enact the various provisions of the Act that affect the ICAC Task Force program, funds have not been appropriated under this section of the Act. Funds have been appropriated for ICACs under other authority—such as the Juvenile Justice and Delinquency Prevention Act (JJDP) (see, e.g., Conference Report accompanying Consolidated Appropriations Act, 2010, H.R. Rep. No. 111-366 at 678 (2009) (directing a specific amount of funds appropriated under sections 404(b) and 405(a) of the JJDP to be made available for the ICAC program)). According to DOJ officials, where OJJDP was able to incorporate Act requirements within current funding levels it has done so (e.g., enhancing data collection).</p> <p>The ICAC Task Force Program received a total of \$50 million in American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, grant funding, which was distributed pursuant to the formula requirements of the PROTECT Our Children Act of 2008. According to DOJ officials, DOJ will use this formula to allocate future appropriations made for the ICAC program and specifically did so in fiscal year 2009 for the 59 ICACs.</p> <p>While the Act did not specify an exact formula for allocating grant monies, it dictated certain considerations that were to be accounted for in allocating funds, for example, the population in each state and number of successful Internet crimes against children prosecutions, among others. Where data were available, OJJDP incorporated these considerations from the Act into its formula for making ICAC funding allocations. However, DOJ officials noted that ICAC funds were not appropriated under this section of the Act, but under other authority.</p> <p>OJJDP awarded \$18,997,913 in grant funding to ICAC task forces in fiscal year 2010.</p> <p>ICAC task forces submit annual applications in response to OJJDP's continuation funding solicitation describing activities to be undertaken with grant funding. According to DOJ officials, these applications are reviewed by OJJDP program management teams who examine the applications</p>

**Appendix II: Status of Efforts of DOJ and
NCMEC's CyberTipline to Implement
Provisions of the PROTECT Our Children Act
of 2008**

Responsible entity or official	Provision	Responsibility	Status of effort
Attorney General	§ 106(d); 42 U.S.C. § 17616(d).	ICAC Program Reporting Requirements: (1) Task forces must submit annual reports to the Attorney General, addressing specific information, such as the number of referrals made by the task force to the U.S. Attorneys office and the number of investigative technical assistance sessions the task force provided, among others. (2) The Attorney General must submit a report to Congress not later than 1 year after enactment on development of the ICAC program and numbers of federal and state investigations, prosecutions and convictions related to child exploitation.	<p>based on financial and programmatic considerations and compare the goals and objectives stated in the application with the requirements outlined in the solicitation. For example, OJJDP officials would review an application to assess the extent to which the ICAC task force would establish a multijurisdictional and multiagency infrastructure to address child exploitation crime.</p> <p>Although ICAC funds have not been appropriated under this section of the PROTECT Our Children Act of 2008, according to DOJ officials, OJJDP prepared reports on the ICAC program in 2009 and in 2010 that included information on the disposition of child exploitation cases and sentencing outcomes, which was a requirement in the Act. At the time the Act was passed, OJJDP did not have a mechanism to capture this information. Therefore, information presented in DOJ annual reports may not include the disposition of all cases in 2009 and 2010.</p>
Attorney General	§ 105(a) – (f); 42 U.S.C. § 17615(a) – (f).	National Internet Crimes Against Children Data System (NIDS): NIDS, to be housed and maintained within DOJ or a credentialed law enforcement agency, is to assist and support law enforcement investigating and prosecuting child exploitation. NIDS, which is required to be available to credentialed law enforcement agencies for a nominal fee, must allow information sharing and case deconfliction, provide a dynamic undercover infrastructure, enable real-time reporting of child exploitation cases involving local victims, identify high-priority suspects, and include a network that provides for secure, online data storage and analysis and online communication, among other things.	<p>According to DOJ officials, the report OJJDP prepared for the Attorney General in 2009 on the status of the ICAC program was incorporated in the National Strategy. The 2010 report on the status of the ICAC program is currently under review at OJJDP, and DOJ officials stated that they plan to incorporate it as part of the update to the National Strategy.</p> <p>DOJ issued a grant solicitation for development of NIDS in March 2009. The initial grant solicitation was for the construction, maintenance, and housing of the system and other tasks, such as linking the system with the ICAC Task Force Portal. In January 2010, applicants for the 2009 NIDS grant solicitation were notified that the agency would not make an award under the solicitation because it planned to pursue a different system for deconfliction and investigation than was described in the solicitation. DOJ reissued the NIDS grant solicitation in June 2010 to select a contractor to conduct a national needs assessment and perform other tasks in support of developing the system in the future. In September 2010, DOJ awarded the grant for the NIDS needs assessment and development activities to the Massachusetts State Police, and its partners Fox Valley Technical College, University of Massachusetts, and University of New Hampshire Crimes Against Children Research Center.</p> <p>According to OJJDP officials, no decision has been made as to where the system will be hosted. The National Coordinator said that the U.S. Marshals</p>

**Appendix II: Status of Efforts of DOJ and
NCMEC's CyberTipline to Implement
Provisions of the PROTECT Our Children Act
of 2008**

Responsible entity or official	Provision	Responsibility	Status of effort
			Service Sex Offender Targeting Center will be considered as an appropriate platform to host the system.
Attorney General	§ 105(g); 42 U.S.C. § 17615(g).	National Internet Crimes Against Children Data System Steering Committee: Requires the Attorney General to establish a Steering Committee to provide guidance to NIDS on the network requirements and assist in the development of strategic plans for NIDS. Includes requirements for the composition of the 10-member committee.	<p>The National Coordinator reported that the NIDS Steering Committee was established in April 2010 with appropriate membership as required by the PROTECT Our Children Act of 2008. The NIDS Steering Committee consists of representatives from ICE, USPIS, FBI, CEOS, OJJDP, and the U.S. Marshals Service, as well as representatives from state and local law enforcement.</p> <p>According to the National Coordinator, the Steering Committee met, but was suspended while DOJ issued a grant solicitation for a NIDS needs assessment. Now that the grantee has been selected, the steering committee has met with the NIDS grantee to discuss formulation and operation of NIDS. The committee plans to provide input to the grantee during the needs assessment process and plans to continue to advise DOJ leadership as to the formulation and operation of NIDS as the system is built and becomes operational.</p>
Attorney General	§ 201; 42 U.S.C. § 17631.	Additional Regional Computer Forensic Labs: Requires the Attorney General to establish additional computer forensic capacity to address the current backlog; funds made available under this section for additional capacity must be dedicated to assisting law enforcement agencies in preventing, investigating, and prosecuting internet crimes against children. The location of any new labs must be determined in consultation with specified stakeholders, such as the Director of the FBI and the Regional Computer Forensic Laboratory National Steering Committee, and others. The Attorney General is required to submit a report on how appropriated funds were utilized no later than 1 year after enactment and annually.	<p>Currently, the FBI is in the process of initiating new Regional Computer Forensics Laboratories (RCFL) in Los Angeles and New Mexico, scheduled to begin operations in January 2011 and March 2011, respectively. In 2006, FBI began the process of seeking a nonpersonnel budget enhancement for these RCFLs and received \$6 million in 2008 to build these facilities. To date, the RCFL Program has received no additional funding to initiate these, or any other, RCFLs. FBI has used the base funding of its RCFL National Program to support the 14 existing RCFLs as well as the 2 new RCFLs.</p> <p>In addition, the FBI's Operational Technology Division has initiated multiple efforts both inside and outside of RCFLs to reduce backlogs. These include initiatives such as:</p> <p>The Case Agent Investigative Review system, which provides investigators the ability to review results of digital forensic examinations conducted in an RCFL from an FBI computer terminal.</p> <p>Investigative kiosks that allow law enforcement to extract data from cell phones or loose media in a forensically sound manner and analyze evidence.</p> <p>Expanded use of preview tools to decrease the amount of digital evidence seized and to triage that which is seized for examination.</p>

**Appendix II: Status of Efforts of DOJ and
NCMEC's CyberTipline to Implement
Provisions of the PROTECT Our Children Act
of 2008**

Responsible entity or official	Provision	Responsibility	Status of effort
Attorney General (through the National Institute of Justice)	§ 401.	National Institute of Justice (NIJ) Study of Risk Factors for Assessing Dangerousness: Requires NIJ to prepare a report to identify the investigative factors indicating whether a subject of an online child exploitation investigation poses a high risk of harm to children, in consultation and coordination with specified entities, such as state, local, and federal law enforcement agencies and NCMEC, among others. Report is due not later than 1 year after enactment, and NIJ must present findings and recommendations to the Judiciary Committees.	According to DOJ officials, this report has not been initiated because funds have not been appropriated for this activity under the PROTECT Our Children Act of 2008, and DOJ does not have plans or a time frame to conduct such a study. However, according to the National Coordinator, an examination of how such a study would be conducted would likely be considered by the National Strategy Working Group as it moves forward.
Attorney General NCMEC	§ 501(a); 18 U.S.C. § 2258A.	Reporting Requirements of Electronic Communication Service Providers and Remote Computing Service Providers (ESPs): Amends the criminal code to establish monetary penalties for ESPs that fail to report to the CyberTipline actual knowledge of facts and circumstances from which there is an apparent violation of specified provisions of the criminal code relating to the sexual exploitation of children and child pornography. Enforcement: The Attorney General is responsible for the enforcement of the reporting requirements. Designation of law enforcement agencies: Requires the Attorney General to designate federal law enforcement agencies to which NCMEC will forward the reports. Also requires the Attorney General to designate, in consultation with the Secretary of State, foreign law enforcement agencies, the conditions under which a report may be forwarded to such foreign agencies, and a process for foreign agencies to request assistance from federal law enforcement related to reports forwarded to them by NCMEC. Requires that the Attorney General maintain and make available the list of designated foreign agencies to specified entities, including the Judiciary Committees, and provides the sense of Congress that the	DOJ officials reported that as of December 15, 2010, the agency is not aware of any violations where ESPs failed to report to the CyberTipline and therefore has not taken any enforcement actions under this provision. According to the National Coordinator, DOJ has not yet designated a list of federal law enforcement agencies or a list of foreign law enforcement agencies to which CyberTipline reports may be forwarded. NCMEC officials said that NCMEC forwards CyberTipline reports to federal law enforcement agencies. Additionally, NCMEC currently refers CyberTipline reports to foreign law enforcement agencies through ICE. DOJ officials said that they plan to coordinate with NCMEC to determine how such a formal designation would work best with NCMEC's current process, but has no time frames for doing so. According to NCMEC, as of December 2010 access to NCMEC's CyberTipline reports is limited to 83 virtual private networks (including ICAC task forces and international law enforcement via ICE) and the federal law enforcement agencies that have representatives who liaison with NCMEC to distribute reports for investigative purposes.

**Appendix II: Status of Efforts of DOJ and
NCMEC's CyberTipline to Implement
Provisions of the PROTECT Our Children Act
of 2008**

Responsible entity or official	Provision	Responsibility	Status of effort
		<p>Attorney General and Secretary of State should make a substantial effort to expand the list.</p> <p>Report forwarding: Requires NCMEC to forward reports to the designated federal law enforcement agencies; and allows NCMEC to forward reports to state/local law enforcement agencies, as well as designated foreign law enforcement agencies, subject to conditions established by the Attorney General and with copies provided to specified entities, including the Attorney General and federal law enforcement agencies. Requires NCMEC to inform the ESP as to whether or not the report was forwarded to a foreign law enforcement agency where the ESP made a report as a result of a request by a foreign law enforcement agency. Limits disclosure of reports by NCMEC to these entities and for purposes under § 2258C (below).</p> <p>Disclosure of information: Limits the permitted disclosures by law enforcement agencies of information contained in a report received from NCMEC to specified individuals and purposes.</p> <p>Preservation: Requires ESPs to preserve information submitted in a report to the CyberTipline for 90 days.</p>	
NCMEC	§ 501(a); 18 U.S.C. § 2258C.	<p>Use to Combat Child Pornography of Technical Elements Relating to Images Reported to the CyberTipline: Allows NCMEC to provide to ESPs, and requires NCMEC to provide to federal, state, and local law enforcement involved in the investigation of child pornography crime, elements relating to any apparent child pornography image of an identified child—but not actual images—for the purpose of permitting the ESP to stop further transmission of images and for the investigation of child pornography cases, respectively.</p>	<p>NCMEC has several initiatives to provide law enforcement and ESPs elements relating to apparent child pornography images of an identified child. For example, according to NCMEC officials, it has developed an initiative called the Law Enforcement Services Portal, which allows law enforcement agencies access to NCMEC's Child Recognition and Identification systems to quickly identify hash values of identified child victims. The portal separates out hash values of identified child victims from those who have not been identified so that law enforcement can quickly match hash values they receive during investigations against the database of image information. According to NCMEC officials, the Law Enforcement Services Portal is operational and efforts to register additional law enforcement officers will continue in 2011.</p> <p>NCMEC established its Hash Value Sharing initiative</p>

**Appendix II: Status of Efforts of DOJ and
NCMEC's CyberTipline to Implement
Provisions of the PROTECT Our Children Act
of 2008**

Responsible entity or official	Provision	Responsibility	Status of effort
			<p>In 2008 to provide elements relating to apparent child pornography images of an identified child. NCMEC provides a list of hash values to requesting ESPs who use hash-seeking software to detect and remove illegal files from their systems. NCMEC provided hash values to 10 ESPs, as of November 23, 2010.</p> <p>In addition, NCMEC established its Uniform Resource Locator (URL) initiative in 2008. Through this initiative, NCMEC provides a daily list of active URLs (also known as Web addresses) that contain photos or videos of apparent child pornography, and, as of November 23, 2010, has provided this list of URLs to 85 ESPs. ESPs may take action to prevent users from accessing these sites. For example, ESPs that host Web sites can check the URL list to ensure that none of the sites that they host are on the list.</p> <p>Under its Child Victim Identification Program, NCMEC requests that when a federal, state, or local law enforcement agency has identified child victims featured in child pornography images that it provides NCMEC with copies of the images and information related to the investigation. NCMEC uses this information to assist law enforcement agencies and prosecutors with determining if submitted images contain children who have been identified in past investigations. Under this program, NCMEC also helps prosecutors prove that a real child is depicted in child pornography images. According to NCMEC, through this effort, children have been rescued from ongoing exploitation as a result of the cooperative efforts between the program and law enforcement.</p>
NCMEC	§ 501(a); 42 U.S.C. § 2258D(d).	Minimizing Access: Requires NCMEC to minimize the number of employees who are provided access to any image provided under § 2258A and ensure that any such image is permanently destroyed upon notification from a law enforcement agency.	<p>According to NCMEC officials, since the passage of the Act NCMEC has reduced the number of employees with access to CyberTipline images by 21 percent from 72 to 57 by removing access to images from employees who transfer from the NCMEC's Exploited Child Division, which reviews CyberTipline reports, to other divisions. Another means that NCMEC has used to minimize the number of employees with access to CyberTipline images is to create a "read only" level of access to the CyberTipline for employees whose job responsibilities require them to have access to CyberTipline information, but not images. Currently, a total of 86 employees have "read only" access.</p> <p>NCMEC officials stated that NCMEC has never been asked by a law enforcement agency to permanently destroy images.</p>

**Appendix II: Status of Efforts of DOJ and
NCMEC's CyberTipline to Implement
Provisions of the PROTECT Our Children Act
of 2008**

Responsible entity or official	Provision	Responsibility	Status of effort
Attorney General	§ 502(a).	Attorney General Report on Implementation, Investigative Methods and Information Sharing: Requires the Attorney General to submit a report to the Judiciary Committees, not later than 12 months after enactment, on the structure established in response to the Act, legal and constitutional implications of the structure, privacy safeguards, and numerical information related to §§ 2258A(b) and 2258C.	According to officials, DOJ has not prepared this report and does not yet have a time frame for completing it.

Source: The PROTECT Our Children Act of 2008 and GAO analysis of information from DOJ and NCMEC.

^aHash values, also known as digital fingerprints, are computational values that serve as unique identifiers for electronic files, such as images, documents, or storage media such as hard drives.

Appendix III: Overview of NIDS Components and System Functions Outlined by the PROTECT Our Children Act of 2008

Table 16 provides an overview of the technical specifications of the National Internet Crimes Against Children Data System (NIDS) as described by the PROTECT Our Children Act of 2008.¹

Table 16: Information on the NIDS Components Required by and Functions Described in the PROTECT Our Children Act of 2008

NIDS components	NIDS functional description
Case deconfliction	NIDS is to provide a secure, online system for federal law enforcement agencies; ICAC task forces; and other state, local, and tribal law enforcement agencies to use in resolving case conflicts.
Real-time reporting	NIDS is required to ensure that child exploitation cases involving local child victims that are reasonably detectable using available software and data are, immediately upon their detection, made available to participating law enforcement agencies.
High-priority suspects identification	Every 30 days, at a minimum, NIDS shall— (1) identify high-priority suspects, such as suspects determined by the volume of suspected criminal activity or other indicators of seriousness of offense or dangerousness to the community or a potential local victim; and (2) report all such identified high-priority suspects to participating law enforcement agencies.
Data collection and analysis	NIDS is required to ensure the availability of any statistical data indicating the overall magnitude of child pornography trafficking and child exploitation in the United States and internationally, such as the number of computers and users engaged in peer-to-peer child pornography, among other data.
Local data analysis	NIDS is to provide a secure online data storage and analysis system that credentialed users may use.
Secure connections	NIDS is required to provide secure connections with state, local, and tribal law enforcement computer networks, consistent with reasonable and established security protocols and guidelines.
Dynamic undercover infrastructure	NIDS is to provide for a dynamic undercover infrastructure to facilitate online investigations of child exploitation.
Software development and support	NIDS is required to facilitate and develop essential software and network capability for law enforcement participants, as well as provide software or direct hosting and support for online investigations of child exploitation activities.
Online communications and collaboration	NIDS must provide for a secure system enabling online communications and collaboration by participants regarding ongoing investigations, investigatory techniques, and best practices.
Guidelines and training and technical assistance	NIDS must provide for guidelines as well as training and technical assistance on use of the system.

Source: PROTECT Our Children Act of 2008.

¹Pub. L. No. 110-401, § 105, 122 Stat. 4229, 4236 (2008).

Appendix IV: Comments from the Department of Justice



U.S. Department of Justice

Office of the Deputy Attorney General

Washington, D.C. 20530

March 25, 2011

Ms. Eileen R. Larence
Director, Homeland Security and Justice
United States Government Accountability Office
Washington, DC 20548

Dear Ms. Larence:

The Department has reviewed the Government Accountability Office's (GAO) draft report entitled "*Combating Child Pornography: Steps Needed to Ensure Tips to Law Enforcement are Useful and Forensic Examinations are Cost Effective*," GAO-11-334. We appreciate GAO's acknowledgment of the progress made under the Act: specifically, the creation and implementation of the *National Strategy*; formal establishment of 61 ICAC task forces; selection of the National Coordinator; and, implementation of the *National Strategy*. The Department generally concurs with the GAO's recommendations and will provide updates to Congress on our progress in implementing them.

In its draft report, GAO notes that three provisions of the Act require additional work to implement. As noted below, activity related to each provision is ongoing. One provision of the Act requires the National Institute of Justice ("NIJ") to complete a report identifying factors that indicate levels of dangerousness of online offenders. Toward that end, the Department solicited grant applications related to the design of the National Internet Crimes Against Children Data System ("NIDS"). The grantee team will provide the Department with three products: 1) an assessment of what is needed to build a system providing law enforcement with information sharing and deconfliction tools; 2) new undercover investigative tools; and 3) a white paper addressing the dangerousness issue with recommendations on further research paths. The latter will allow the Department to determine the appropriate avenue to direct research grants for further study of this complex issue and will assist in identifying the factors contemplated by the Act. The grant was awarded in September 2010, and these three products will be delivered by August 31, 2012.

GAO also noted that the Department has not completed work on that provision of the Act related to information sharing structures. As noted above, the Department solicited grant applications for the design of an information sharing system, and when the system is closer to fruition, the Department will report to Congress on its progress.

Finally, with respect to that portion of the Act requiring the designation of foreign law enforcement agencies to receive CyberTips from the National Center for Missing and Exploited Children ("NCMEC"), a working group has been established, which includes various law enforcement agencies and NCMEC, and is working to satisfy this provision. We expect to be able to report on substantial progress on this provision of the Act to Congress in the next six months.

Appendix IV: Comments from the Department
of Justice

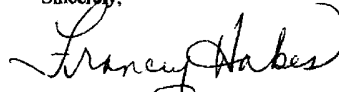
With respect to the three remaining recommendations, the Department concurs with GAO. One recommendation is that NCMEC enhance its ability to collect feedback from law enforcement on the efficacy of the CyberTips it distributes to law enforcement. Efforts to improve the CyberTip process are underway, and NCMEC and the Department will be able to report to Congress on these improvements in the next six months. GAO also recommended that the Department build the National Internet Crimes Against Children Data System, as required in the Protect Our Children Act of 2008. We concur, and as noted above, are in process of receiving a needs assessment on the system from a qualified team of grantees. We also agree with the recommendation that the efficacy of computer forensic process should be assessed. There are two major efforts currently underway to review and assess digital forensics across the Department.

The GAO has recommended that the Attorney General direct the National Strategy Working Group and its Technical Assistance Subcommittee to assess the efficacy of various steps federal law enforcement agencies take that they believe enhances the integrity of forensic analysis of digital evidence in investigating online child pornography crimes. The Subcommittee has been studying the issue of the timeliness and usefulness of computer forensic examinations and has made recommendations that are currently under review.

In addition to the work of the above-referenced Subcommittee, the Office of the Deputy Attorney General leads a Computer Forensics Working Group. This group is also examining the current processes by which the Department conducts its digital forensics examinations. As part of these reviews, the Department will be taking into account the resources associated with various steps DOJ law enforcement takes in conducting digital forensic analysis. We hope to be able to provide an update to Congress on our progress on digital forensics in the next six months.

The Department appreciates the work of the GAO and this opportunity to comment on the GAO's draft report. Should you have any questions regarding this topic, please do not hesitate to contact Richard Theis, Department of Justice Audit Liaison on 202-514-0469.

Sincerely,



Francey Hakes
National Coordinator for Child Exploitation
Prevention and Interdiction

Appendix V: Comments from the National Center for Missing and Exploited Children



Charles B. Wang International
Children's Building
699 Prince Street
Alexandria, VA 22314-3175
U.S.A.

Telephone 703.224.2150

Facsimile 703.224.2122

www.missingkids.com

www.cybertipline.com

Other Offices
California
Florida
New York
Texas

March 22, 2011

Eileen R. Larance
Director, Homeland Security and Justice
United States Government Accountability Office
Washington, DC

Dear Ms. Larance:

The National Center for Missing & Exploited Children (NCMEC) was pleased to work with your staff for the report entitled "Combating Child Pornography: Steps Needed to Ensure Tips to Law Enforcement are Useful and Forensic Examinations are Cost Effective", GAO-11-334. As noted in the report, NCMEC will further its efforts to solicit better feedback from law enforcement on the usefulness of individual CyberTipline reports. We agree there should be a better understanding of how information provided by electronic communication service providers, pursuant to 18 U.S.C. §2258A, may determine whether a law enforcement agency can begin an investigation.

We appreciate the GAO's recognition that NCMEC has played a key role in coordinating law enforcement efforts through the operation of the CyberTipline. NCMEC will continue to meet with stakeholders to explore ways to improve the overall CyberTipline process.

Thank you very much.

A handwritten signature in cursive script that reads "Ernie Allen".

Ernie Allen
President and Chief Executive Officer

Appendix VI: GAO Contact and Acknowledgments

GAO Contact

Eileen R. Larence, (202) 512-8777 or larencee@gao.gov

Acknowledgments

In addition to the contact named above, Mary Catherine Hult, Assistant Director, and Robert Rivas, Analyst-in-Charge, managed this assignment. David Alexander, Kristy Brown, Amy Bush, Christopher Conrad, Katherine Davis, Pawnee A. Davis, Lorraine Ettaro, Harold Lewis, Marvin McGill, Gary Mountjoy, Susan Sachs, and Janet Temko made significant contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

